

1 The access terminal shall add a pilot to the Candidate Set if one of the following conditions  
 2 is met:

- 3 • Pilot is not already in the Active Set or Candidate Set and the strength of the pilot  
 4 exceeds the value specified by PilotAdd.
- 5 • Pilot is deleted from the Active Set, its pilot drop timer has expired,  
 6 DynamicThresholds is equal to '1', and the pilot strength is above the threshold  
 7 specified by PilotDrop.
- 8 • Pilot is deleted from the Active Set but its pilot drop timer has not expired.

9 The access terminal shall delete a pilot from the Candidate Set if one of the following  
 10 conditions is met:

- 11 • Pilot is added to the Active Set.
- 12 • Pilot's drop timer has expires.
- 13 • Pilot is added to the Candidate Set; and, as a consequence, the size of the Candidate  
 14 Set exceeds  $N_{RUPCandidate}$ . In this case, the access terminal shall delete the weakest  
 15 pilot in the set. Pilot A is considered weaker than pilot B:
  - 16 – If pilot A has an active drop timer but pilot B does not,
  - 17 – If both pilots have an active drop timer and pilot A's drop timer is closer to  
 18 expiration than pilot B's, or
  - 19 – If neither of the pilots has an active drop timer and pilot A's strength is less than  
 20 pilot B's.

#### 21 6.6.5.3.7 Neighbor Set Management

22 The access terminal shall support a minimum Neighbor Set size of  $N_{RUPNeighbor}$  pilots.

23 Upon receiving the first *OverheadMessages.Updated* indication since transitioning out of  
 24 the Inactive State, the access terminal shall initialize the Neighbor Set to the list of  
 25 neighbors pilots given as public data by the Overhead Messages Protocol.

26 The access terminal shall implement a "least recently used" scheme for pilots in the  
 27 Neighbor Set as follows.

28 The access terminal shall maintain a counter, AGE, for each pilot in the Neighbor Set. The  
 29 initial setting of this counter depends on what set the pilot was in before it became a  
 30 member of the Neighbor Set:

- 31 • For pilots that were deleted from the Active Set or Candidate Set, the access terminal  
 32 shall set AGE to 0 when adding these pilots to the Neighbor Set.
- 33 • For pilots that were deleted from the Remaining Set, the access terminal shall set  
 34 AGE to NeighborMaxAge when adding these pilots to the Neighbor Set.
- 35 • When the access terminal initializes the Neighbor Set, it shall set AGE to  
 36 NeighborMaxAge for each pilot in the set.

1 The access terminal shall increment AGE for every pilot in the Neighbor Set each time  
2 either of the following occurs:

- 3 • The access terminal receives an *OverheadMessages.Updated* indication and the  
4 public data of the Overhead Messages Protocol contains a neighbor list that is not  
5 identical to the list provided previously as public data by the Overhead Messages  
6 Protocol , or
- 7 • The access terminal receives a NeighborList message listing a neighbor list that is not  
8 identical to the list specified in the previous (if any) NeighborList message.

9 The access terminal shall add a pilot to the Neighbor Set if:

- 10 • The pilot was deleted from the Active Set with an expired pilot drop timer.
- 11 • The pilot drop timer of a pilot in the Candidate Set expires.
- 12 • The pilot was a member of the Remaining Set, and it was either provided as public  
13 data by the Overhead Messages Protocol or it was listed in a received NeighborList  
14 message. The access terminal shall add the pilots listed in the message in the order  
15 they are listed, and shall only add the pilots to the Neighbor Set if, after adding them  
16 and deleting the appropriate pilots, the size of the Neighbor Set does not exceed  
17  $N_{RUPNeighbor}$ .

18 The access terminal shall delete a pilot from the Neighbor Set if:

- 19 • The Pilot is added to the Active Set or Candidate Set, or if the AGE of the pilot  
20 exceeds NeighborMaxAge and the size of the Neighbor Set exceeds  $N_{RUPNeighbor}$  due to  
21 new additions.

22 If there are more pilots with AGE exceeding NeighborMaxAge than needed to make room for  
23 new additions to the Neighbor Set, the pilot with the highest AGE shall be deleted first.

24 The access terminal shall perform the procedures specified in 6.6.5.3.1 if a plot (specified by  
25 the pilot's PN offset and the pilot's CDMA Channel) is added to or deleted from the Neighbor  
26 Set.

#### 27 6.6.5.3.8 Remaining Set Management

28 The access terminal shall initialize the Remaining Set to contain all the pilots whose PN  
29 offset index is an integer multiple of PilotIncrement and are not already members of any  
30 other set.

31 The access terminal shall add a pilot to the Remaining Set if it deletes the pilot from the  
32 Neighbor Set and if the pilot was not added to the Active Set or Candidate Set.

33 The access terminal shall delete the pilot from the Remaining Set if it adds it to another set.

#### 34 6.6.5.3.9 Pilot PN Phase Measurement

35 The access terminal shall measure the arrival time, PILOT\_ARRIVAL, for each pilot reported  
36 to the access network. The pilot arrival time shall be the time of occurrence, as measured at  
37 the access terminal antenna connector, of the earliest arriving usable multipath component  
38 of the pilot. The arrival time shall be measured relative to the access terminal's time

1 reference in units of PN chips. The access terminal shall compute the reported pilot PN  
 2 phase, PILOT\_PN\_PHASE, as:

$$3 \quad \text{PILOT\_PN\_PHASE} = (\text{PILOT\_ARRIVAL} + (64 \times \text{PILOT\_PN})) \bmod 2^{15},$$

4 where PILOT\_PN is the PN sequence offset index of the pilot.

5 **6.6.5.4 Message Sequence Numbers**

6 The access network shall validate all received RouteUpdate messages as specified in  
 7 6.6.5.4.1.

8 The access terminal shall validate all received TrafficChannelAssignment messages as  
 9 specified in 6.6.5.4.2.

10 The RouteUpdate message and the TrafficChannelAssignment message carry a  
 11 MessageSequence field that serves to flag duplicate or stale messages.

12 The MessageSequence field of the RouteUpdate message is independent of the  
 13 MessageSequence field of the TrafficChannelAssignment message.

14 **6.6.5.4.1 RouteUpdate Message Validation**

15 When the access terminal first sends a RouteUpdate message, it shall set the  
 16 MessageSequence field of the message to zero. Subsequently, the access terminal shall  
 17 increment this field each time it sends a RouteUpdate message.

18 The access network shall consider all RouteUpdate messages it receives in the Idle State as  
 19 valid.

20 The access network shall initialize the receive pointer,  $V(R)$  to the MessageSequence field of  
 21 the first RouteUpdate message it received in the Idle State, and the access network shall  
 22 subsequently set it to the MessageSequence field of each received RouteUpdate message.

23 When the access network receives a RouteUpdate message in the Connected State, it shall  
 24 validate the message using the procedure defined in 10.6. The access network shall discard  
 25 the message if it is stale.

26 **6.6.5.4.2 TrafficChannelAssignment Message Validation**

27 The access network shall set the MessageSequence field of the TrafficChannelAssignment  
 28 message it sends in the Idle State to zero. Subsequently, each time the access network  
 29 sends a new TrafficChannelAssignment message in the Connected State, it shall increment  
 30 this field. If the access network is sending the same message multiple times, it shall not  
 31 change the value of this field between transmissions.<sup>23</sup>

32 The access terminal shall initialize a receive pointer,  $V(R)$  to the MessageSequence field of  
 33 the TrafficChannelAssignment message that it receives in the Idle State.

---

<sup>23</sup> The access network may send a message multiple times to increase its delivery probability.

1 When the access terminal receives a TrafficChannelAssignment message, it shall validate  
2 the message using the procedure defined in 10.6. The access terminal shall discard the  
3 message if it is stale.

4 6.6.5.5 Idle State

5 The Idle State corresponds to the Air Link Management Protocol Idle State.

6 In this state, RouteUpdate messages from the access terminal are based on the distance  
7 between the sector where the access terminal last sent a RouteUpdate message and the  
8 sector currently in its active set.

9 The access network sends the TrafficChannelAssignment message to open a connection in  
10 this state.

11 Upon entering this state, the access terminal shall remove all Neighbor structures from  
12 NeighborListMessageNeighborList and perform the procedures specified in 6.6.5.3.1.

13 6.6.5.5.1 Active Set Maintenance

14 The access network shall not initially maintain an Active Set for the access terminal in this  
15 state.

16 If the access network receives an *Open* command, it shall initialize the Active Set to the set  
17 of pilots it sends in the TrafficChannelAssignment message, sent in response to the  
18 command (see 6.6.5.2.3).

19 The access terminal shall initially keep an Active Set of size one when it is in the Idle State.  
20 The Active Set pilot shall be the pilot associated with the Control Channel the access  
21 terminal is currently monitoring. The access terminal shall send an *IdleHO* indication when  
22 the Active Set changes in the Idle State.

23 The access terminal shall not change its Active Set pilot at a time that causes it to miss a  
24 synchronous Control Channel capsule. Other rules governing when to replace this Active  
25 Set pilot are beyond the scope of this specification.

26 If the access terminal receives a TrafficChannelAssignment message, it shall set its Active  
27 Set to the list of pilots specified in the message.

28 6.6.5.5.2 Pilot Channel Supervision in the Idle State

29 The access terminal shall perform pilot channel supervision in the Idle State as follows:

- 30 • Access terminal shall monitor the pilot strength of the pilot in its active set, all the  
31 pilots in the candidate set and all the pilots in the neighbor set that are on the same  
32 frequency.
- 33 • If the strength of all the pilots that the access terminal is monitoring goes below the  
34 value specified by PilotDrop, the access terminal shall start a pilot supervision timer  
35 for  $T_{RUPPilotSupervision}$  seconds.
- 36 • If the strength of at least one of the pilots goes above the value specified by PilotDrop  
37 while the pilot supervision timer is counting down, the access terminal shall stop the  
38 timer.

- 1     • If the pilot supervision timer expires, the access terminal shall return a *NetworkLost*  
2        indication.

3     6.6.5.5.3 Processing the TrafficChannelAssignment Message in the Idle State

4     If the access terminal receives a TrafficChannelAssignment message in this state, it shall  
5        update its Active Set as described above, and perform the following:

- 6     • If the Channel Record is included in the message, the access terminal shall set  
7        CurrentFrequency to the current CDMA channel.
- 8     • Start a connection timer for  $T_{RUPConnectionSetup}$  seconds.
- 9     • Issue the following commands:  
10        – *ReverseTrafficChannelMAC.Activate*  
11        – *ForwardTrafficChannelMAC.Activate*
- 12     • If the protocol receives a *ReverseTrafficChannelMAC.LinkAcquired* indication the  
13        access terminal shall:  
14           – Send a TrafficChannelComplete message with the MessageSequence field of the  
15            message set to the MessageSequence field of the TrafficChannelAssignment  
16            message.  
17           – Disable the connection timer.  
18           – Transition to the Connected State.

19     If the connection timer expires the access terminal shall perform the following:

- 20     • Issue a *ReverseTrafficChannelMAC.Deactivate* command.
- 21     • Issue a *ForwardTrafficChannelMAC.Deactivate* command.
- 22     • If as a result of processing the TrafficChannelAssignment message the access  
23        terminal has tuned to a different frequency, the access terminal shall return back to  
24        the frequency that is was monitoring prior to processing of the  
25        TrafficChannelAssignment message.

26     6.6.5.5.4 Route Update Report Rules

27     The access terminal shall send RouteUpdate messages to update its location with the  
28        access network.

29     The access terminal shall not send a RouteUpdate message if the connection timer is active.

30     The access terminal shall comply with the following rules when sending RouteUpdate  
31        messages.

- 32     • The access terminal shall send a RouteUpdate message whenever it transmits on  
33        the Access Channel.
- 34     • The access terminal shall include in the RouteUpdate message the pilot PN phase,  
35        pilot strength, and drop timer status for every pilot in the Active Set and Candidate  
36        Set.

- 1     • The access terminal shall send a RouteUpdate message if the computed value  $r$  is  
 2       greater than the value provided in the RouteUpdateRadius field of the  
 3       SectorParameters message transmitted by the sector in which the access terminal  
 4       last sent a RouteUpdate message.

5       If  $(x_L, y_L)$  are the longitude and latitude of the sector in whose coverage area the  
 6       access terminal last sent a RouteUpdate, and  $(x_C, y_C)$  are the longitude and latitude  
 7       of the sector currently providing coverage to the access terminal, then  $r$  is given by<sup>24</sup>

$$r = \left\lfloor \frac{\sqrt{[(x_C - x_L) \times \cos(\frac{\pi}{180} \times \frac{y_L}{14400})]^2 + [y_C - y_L]^2}}{16} \right\rfloor$$

9       The access terminal shall compute  $r$  with an error of no more than  $\pm 5\%$  of its true  
 10      value when  $|y_L/14400|$  is less than 60 and with an error of no more than  $\pm 7\%$  of its  
 11      true value when  $|y_L/14400|$  is between 60 and 70.<sup>25</sup>

12     6.6.5.6 Connected State

13       The Connected State corresponds to the Air Link Management Protocol Connected State.

14       In this state, RouteUpdate messages from the access terminal are based on changes in the  
 15       radio link between the access terminal and the access network, obtained through pilot  
 16       strength measurements at the access terminal.

17       The access network determines the contents of the Active Set through  
 18       TrafficChannelAssignment messages.

19     6.6.5.6.1 Active Set Maintenance

20       6.6.5.6.1.1 Access Network

21       Whenever the access network sends a TrafficChannelAssignment message to the access  
 22       terminal, it shall add to the Active Set any pilots listed in the message that are not  
 23       currently in the Active Set.

24       The access network shall delete a pilot from the Active Set if the pilot was not listed in a  
 25       TrafficChannelAssignment message and if the access network received the  
 26       TrafficChannelComplete message, acknowledging that TrafficChannelAssignment message.

27       The access network should send a TrafficChannelAssignment message to the access  
 28       terminal in response to changing radio link conditions, as reported in the access terminal's  
 29       RouteUpdate messages.

<sup>24</sup> The  $x$ 's denote longitude and the  $y$ 's denote latitude.

<sup>25</sup>  $x_L$  and  $y_L$  are given in units of 1/4 seconds.  $x_L/14400$  and  $y_L/14400$  are in units of degrees.

1 The access network should only specify a pilot in the TrafficChannelAssignment message if  
 2 it has allocated the required resources in the associated sector. This means that the sector  
 3 specified by the pilot is ready to receive data from the access terminal and is ready to  
 4 transmit queued data to the access terminal should the access terminal point its DRC at  
 5 that sector.

6 If the access network adds or deletes a pilot in the Active Set, it shall send an  
 7 *ActiveSetUpdated* indication.

8 If the access network adds a pilot specified in a RouteUpdate message to the Active Set, the  
 9 access network may use the PilotPNPhase field provided in the message to obtain a round  
 10 trip delay estimate from the access terminal to the sector associated with this pilot. The  
 11 access network may use this estimate to accelerate the acquisition of the access terminal's  
 12 Reverse Traffic Channel in that sector.

#### 13 6.6.5.6.1.2 Access Terminal

14 If the access terminal receives a valid TrafficChannelAssignment message (see 6.6.5.4.2), it  
 15 shall replace the contents of its current Active Set with the pilots specified in the message.  
 16 The access terminal shall process the message as defined in 6.6.5.6.4.

#### 17 6.6.5.6.2 ResetReport Message

18 The access network may send a ResetReport message to reset the conditions under which  
 19 RouteUpdate messages are sent from the access terminal. Access terminal usage of the  
 20 ResetReport message is specified in the following section.

#### 21 6.6.5.6.3 Route Update Report Rules

22 The access terminal sends a RouteUpdate message to the access network in this state to  
 23 request addition or deletion of pilots from its Active Set. The access terminal shall send the  
 24 message if any one of the following occurs:

- 25 • If DynamicThresholds is equal to '0' and the strength of a Neighbor Set or Remaining  
   26 Set pilot is greater than the value specified by PilotAdd.
- 27 • If DynamicThresholds is equal to '1' and the strength of a Neighbor Set or Remaining  
   28 Set pilot, PS, satisfies the following inequality:

$$29 \quad 10 \times \log_{10} PS > \max \left( \frac{\text{SoftSlope}}{8} \times 10 \times \log_{10} \sum_{i \in A} PS_i + \frac{\text{AddIntercept}}{2}, -\frac{\text{PilotAdd}}{2} \right)$$

30 where the summation is performed over all pilots currently in the Active Set.

- 31 • If DynamicThresholds is equal to '0' and the strength of a Candidate Set pilot is  
   32 greater than the value specified by PilotCompare above an Active Set pilot, and a  
   33 RouteUpdate message carrying this information has not been sent since the last  
   34 ResetReport message was received.
- 35 • If DynamicThresholds is equal to '1' and

- 36 – the strength of a Candidate Set pilot, PS, satisfies the following inequality:

$$10 \times \log_{10} PS > \frac{\text{SoftSlope}}{8} \times 10 \times \log_{10} \sum_{i \in A} PS_i + \frac{\text{AddIntercept}}{2}$$

2 where the summation is performed over all pilots currently in the Active Set, and

- 3 – a RouteUpdate message carrying this information has not been sent since the last  
 4 ResetReport message was received.

- 5 • If DynamicThresholds is equal to '1' and

- 6 – the strength of a Candidate Set pilot is greater than the value specified by  
 7 PilotCompare above an Active Set pilot, and

- 8 – the strength of a Candidate Set pilot, PS, satisfies the following inequality:

$$9 \quad 10 \times \log_{10} PS > \frac{\text{SoftSlope}}{8} \times 10 \times \log_{10} \sum_{i \in A} PS_i + \frac{\text{AddIntercept}}{2}$$

10 where the summation is performed over all pilots currently in the Active Set, and

- 11 – a RouteUpdate message carrying this information has not been sent since the last  
 12 ResetReport message was received.

- 13 • The pilot drop timer of an Active Set pilot has expired, and a RouteUpdate message  
 14 carrying this information has not been sent since the last ResetReport message was  
 15 received.

#### 16 6.6.5.6.4 Processing the TrafficChannelAssignment Message

17 The access terminal shall process a valid TrafficChannelAssignment (see 6.6.5.4.2) message  
 18 as follows:

- 19 • If the TrafficChannelAssignment message contains a value for the FrameOffset that is  
 20 different from the value of the FrameOffset received in the last  
 21 TrafficChannelAssignment message that was received in the Idle state, then the  
 22 access terminal shall return a *RouteUpdate.AssignmentRejected* indication and shall  
 23 discard the message.
- 24 • The access terminal shall update its Active Set as defined in 6.6.5.6.1.2.
- 25 • The access terminal shall tune to the frequency defined by the Channel record, if this  
 26 record is included in the message.
- 27 • The access terminal shall start monitoring and responding to the Power Control  
 28 Channels defined by the MACIndex fields provided in the message. The access  
 29 terminal should use the SofterHandoff fields to identify the Power Control Channels  
 30 that are carrying identical information and can therefore be soft-combined.
- 31 • The access terminal shall send the access network a TrafficChannelComplete  
 32 message specifying the MessageSequence value received in the  
 33 TrafficChannelAssignment message.

1        6.6.5.6.5 Processing the TrafficChannelComplete Message

2        The access network should set a transaction timer when it sends a  
 3        TrafficChannelAssignment message. If the access network sets a transaction timer, it shall  
 4        reset the timer when it receives a TrafficChannelComplete message containing a  
 5        MessageSequence field equal to the one sent in the TrafficChannelAssignment message.

6        If the timer expires, the access network should return a *RouteUpdate.ConnectionLost*  
 7        indication.

8        6.6.5.6.6 Transmission and Processing of the NeighborList Message

9        The access network may send the NeighborList message to the access terminal when the  
 10      protocol is in the Connected State to override the search window size and/or search window  
 11      offset corresponding to a pilot in the Neighbor Set.

12      Upon receiving a NeighborList message, the access terminal shall perform the following in  
 13      the order specified:

- 14        • The access terminal shall remove all Neighbor structures from  
                 NeighborListMessageNeighborList.
- 16        • For each pilot (specified by its pilot PN and its channel) listed in the received  
                 NeighborList message, the access terminal shall add a Neighbor structure to  
                 NeighborListMessageNeighborList and populate it as follows:
  - 19            – Set the structure's PilotPN field to the message's corresponding PilotPN field.
  - 20            – If the message's ChannelIncluded field is set to '1', set the structure's Channel  
                   field to the message's corresponding Channel field. Otherwise, set the structure's  
                   Channel field to the current channel.
  - 23            – If the message's SearchWindowSizeIncluded field is set to '1', then set the  
                   structure's SearchWindowSize field to the message's corresponding  
                   SearchWindowSize field. Otherwise, set the structure's SearchWindowSize field to  
                   NULL.
  - 27            – If the SearchWindowOffsetIncluded field is set to '1', then set the structure's  
                   SearchWindowOffset field to the message's corresponding SearchWindowOffset  
                   field. Otherwise, set the structure's SearchWindowOffset field to NULL.
- 30        • Perform the procedures specified in 6.6.5.3.1.

31        6.6.5.6.7 Processing of OverheadMessages.Updated Indication

32      Upon receiving *OverheadMessages.Updated* indication, the access terminal shall perform  
 33      the following:

- 34        • The access terminal shall remove all Neighbor structures from the  
                 OverheadMessagesNeighborList list.
- 36        • For each pilot (specified by its pilot PN and its channel) in the neighbor list given as  
                 public data of Overhead Messages Protocol, the access terminal shall add a Neighbor  
                 structure to the OverheadMessagesNeighborList list and populate it as follows:

- 1   – Set the structure's PilotPN field to the corresponding NeighborPilotPN field given as  
2   public data of the Overhead Messages Protocol.
- 3   – If the Overhead Messages Protocol's NeighborChannelIncluded field is set to '1', set  
4   the structure's Channel field to the Overhead Messages Protocol's corresponding  
5   NeighborChannel. Otherwise, set the structure's Channel field to the current  
6   channel.
- 7   – If the Overhead Messages Protocol's SearchWindowSizeIncluded field is set to '1',  
8   then set the structure's SearchWindowSize field to the Overhead Messages  
9   Protocol's corresponding SearchWindowSize field. Otherwise, set the structure's  
10   SearchWindowSize field to NULL.
- 11   – If the Overhead Messages Protocol's SearchWindowOffsetIncluded field is set to '1',  
12   then set the structure's SearchWindowOffset field to the Overhead Messages  
13   Protocol's corresponding SearchWindowOffset field. Otherwise, set the structure's  
14   SearchWindowOffset field to NULL.
- 15   • Perform the procedures specified in 6.6.5.3.1.

16   **6.6.6 Message Formats**

17   **6.6.6.1 RouteUpdate**

18   The access terminal sends the RouteUpdate message to notify the access network of its  
19   current location and provide it with an estimate of its surrounding radio link conditions.  
20

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
MessageSequence	8
ReferencePilotPN	9
ReferencePilotStrength	6
ReferenceKeep	1
NumPilots	4

NumPilots occurrences of the following three fields:

PilotPNPhase	15
ChannelIncluded	1
Channel	0 or 24
PilotStrength	6
Keep	1

Reserved	Variable
----------	----------

21   **MessageID**

The access terminal shall set this field to 0x00.

1	MessageSequence	The access terminal shall set this field to the sequence number of this message. The sequence number of this message is 1 more than the sequence number of the last RouteUpdate message (modulo $2^8$ ) sent by this access terminal. If this is the first RouteUpdate message sent by the access terminal, it shall set this field to 0x00.
6	ReferencePilotPN	The access terminal shall set this field to the access terminal's time reference (the reference pilot), relative to the zero offset pilot PN sequence in units of 64 PN chips.
9	ReferencePilotStrength	The access terminal shall set this field to $\lfloor -2 \times 10 \times \log_{10}PS \rfloor$ , where PS is the strength of the reference pilot, measured as specified in 6.6.5.3.2. If this value is less than 0, the access terminal shall set this field to '000000'. If this value is greater than '111111', the access terminal shall set this field to '111111'.
15	ReferenceKeep	If the pilot drop timer corresponding to the reference pilot has expired, the access terminal shall set this field to '0'; otherwise, the access terminal shall set this field to '1'.
18	NumPilots	The access terminal shall set this field to the number of pilots that follow this field in the message.
20	PilotPNPhase	The PN offset in resolution of 1 chip of a pilot in the Active Set or Candidate Set of the access terminal that is not the reference pilot.
22	ChannelIncluded	The access terminal shall set this field to '1' if the channel for this pilot offset is not the same as the current channel. Otherwise, the access terminal shall set this field to '0'.
25	Channel	The access terminal shall include this field if the ChannelIncluded field is set to '1'. The access terminal shall set this to the channel record corresponding to this pilot (see 10.1). Otherwise, the access terminal shall omit this field for this pilot offset.
29	PilotStrength	The access terminal shall set this field to $\lfloor -2 \times 10 \times \log_{10}PS \rfloor$ , where PS is the strength of the pilot in the above field, measured as specified in 6.6.5.3.2. If this value is less than 0, the access terminal shall set this field to '000000'. If this value is greater than '111111', the access terminal shall set this field to '111111'.
34	Keep	If the pilot drop timer corresponding to the pilot in the above field has expired, the access terminal shall set this field to '0'; otherwise, the access terminal shall set this field to '1'.

- 1    Reserved                  The number of bits in this field is equal to the number needed to  
 2                                make the message length an integer number of octets. This field shall  
 3                                be set to all zeros.  
 4

<b>Channels</b>	AC	RTC	<b>SLP</b>	Reliable <sup>26</sup>	Best Effort
<b>Addressing</b>		unicast	<b>Priority</b>		20

5    6.6.6.2 TrafficChannelAssignment

6    The access network sends the TrafficChannelAssignment message to manage the access  
 7                                terminal's Active Set.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
MessageSequence	8
ChannelIncluded	1
Channel	0 or 24
FrameOffset	4
DRCLength	2
DRCChannelGain	6
AckChannelGain	6
NumPilots	4

NumPilots occurrences of the following fields

PilotPN	9
SofterHandoff	1
MACIndex	6
DRCCover	3
RABLength	2
RABOffset	3

Reserved	Variable
----------	----------

- 9    MessageID                The access network shall set this field to 0x01.

---

<sup>26</sup> This message is sent reliably when it is sent over the Reverse Traffic Channel.

- 1      MessageSequence      The access network shall set this to 1 higher than the  
 2      MessageSequence field of the last TrafficChannelAssignment message  
 3      (modulo  $2^S$ , S=8) sent to this access terminal.
- 4      ChannelIncluded      The access network shall set this field to '1' if the Channel record is  
 5      included for these pilots. Otherwise, the access network shall set this  
 6      field to '0'.
- 7      Channel      The access network shall include this field if the ChannelIncluded  
 8      field is set to '1'. The access network shall set this to the channel  
 9      record corresponding to this pilot (see 10.1). Otherwise, the access  
 10     network shall omit this field for this pilot offset. If Channel is  
 11     included, the access network shall set the SystemType field of the  
 12     Channel record to '0000'.
- 13     FrameOffset      The access network shall set this field to the frame offset the access  
 14     terminal shall use when transmitting the Reverse Traffic Channel, in  
 15     units of slots.
- 16     DRCLength      The access network shall set this field to the number of slots the  
 17     access terminal shall use to transmit a single DRC value, as shown in  
 18     Table 6.6.6.2-1.

**Table 6.6.6.2-1. DRCLength Encoding**

<b>Field value (binary)</b>	<b>DRCLength (slots)</b>
'00'	1
'01'	2
'10'	4
'11'	8

- 20     DRCChannelGain      The access network shall set this field to the ratio of the power level  
 21     of the DRC Channel (when it is transmitted) to the power level of the  
 22     Reverse Traffic Pilot Channel expressed as 2's complement value in  
 23     units of 0.5 dB. The valid range for this field is from -9 dB to +6 dB,  
 24     inclusive. The access terminal shall support all the values in the  
 25     valid range for this field.
- 26     AckChannelGain      The access network shall set this field to the ratio of the power level  
 27     of the Ack Channel (when it is transmitted) to the power level of the  
 28     Reverse Traffic Pilot Channel expressed as 2's complement value in  
 29     units of 0.5 dB. The valid range for this field is from -3 dB to +6 dB,  
 30     inclusive. The access terminal shall support all the values in  
 31     valid range for this field.

1	NumPilots	The access network shall set this field to the number of pilots included in this message.
2	PilotPN	The access network shall set this field to the PN Offset associated with the sector that will transmit a Power Control Channel to the access terminal, to whom the access terminal is allowed to point its DRC, and whose Control Channel and Forward Traffic Channel the access terminal may monitor.
3	SofterHandoff	If the Forward Traffic Channel associated with this pilot will carry the same closed-loop power control bits as that of the previous pilot in this message, the access network shall set this field to '1'; otherwise, the access network shall set this field to '0'. The access network shall set the first instance of this field to '0'.
4	MACIndex	Medium Access Control Index. The access network shall set this field to the MACIndex assigned to the access terminal by this sector.
5	DRCCover	The access network shall set this field to the index of the DRC cover associated with the sector specified in this record.
6	RABLength	The access network shall set this field to the number of slots over which the Reverse Activity Bit is transmitted, as shown in Table 6.6.6.2-2.

20 **Table 6.6.6.2-2. Encoding of the RABLength Field**

Field value (binary)	RABLength (slots)
'00'	8
'01'	16
'10'	32
'11'	64

21	RABOffset	The access network shall set this field to indicate the slots in which a new Reverse Activity Bit is transmitted by this sector. The value (in slots) of RABOffset is the number the field is set to multiplied by RABLength/8.
22	Reserved	The number of bits in this field is equal to the number needed to make the message length an integer number of octets. This field shall be set to all zeros.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable	Best Effort <sup>27</sup>
<b>Addressing</b>		unicast	<b>Priority</b>		20

## 1    6.6.6.3 TrafficChannelComplete

2    The access terminal sends the TrafficChannelComplete message to provide an  
3    acknowledgement for the TrafficChannelAssignment message.

4

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
MessageSequence	8

5    MessageID                 The access terminal shall set this field to 0x02.

6    MessageSequence         The access terminal shall set this field to the MessageSequence field  
7                                 of the TrafficChannelAssignment message whose receipt this message  
8                                 is acknowledging.

<b>Channels</b>	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

## 10    6.6.6.4 ResetReport

11    The access network sends the ResetReport message to reset the RouteUpdate transmission  
12    rules at the access terminal.

13

<b>Field</b>	<b>Length (bits)</b>
MessageID	8

14    MessageID                 The access network shall set this field to 0x03.

15

---

<sup>27</sup> The TrafficChannelAssignment message sent in response to the Open command is sent using best effort SLP. All subsequent TrafficChannelAssignment messages are sent using reliable delivery SLP.

<b>Channels</b>	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

## 1    6.6.6.5 NeighborList

2    The NeighborList message is used to convey information corresponding to the neighboring  
3    sectors to the access terminals when the access terminal is in the Connected State.

4

Field	Length (bits)
MessageID	8
Count	5

Count occurrences of the following field:

PilotPN	9
---------	---

Count occurrences of the following two fields:

ChannelIncluded	1
Channel	0 or 24

SearchWindowSizeIncluded	1
--------------------------	---

Count occurrences of the following field

SearchWindowSize	0 or 4
------------------	--------

SearchWindowOffsetIncluded	1
----------------------------	---

Count occurrences of the following field

SearchWindowOffset	0 or 3
--------------------	--------

Reserved	Variable
----------	----------

5    MessageID                 The access network shall set this field to 0x04.

6    Count                      The access network shall set this field to the number of records  
7                                specifying neighboring sectors information included in this message.8    PilotPN                   The access network shall set this field to the PN Offset of a  
9                                neighboring sector for which the access network is providing search  
10                              window information in this message.11   ChannelIncluded          The access network shall set this field to ‘1’ if a Channel record is  
12                                included for this neighbor, and to ‘0’ otherwise. The access network

1 shall omit this field if the corresponding NeighborChannelIncluded  
2 field is set to '0'. Otherwise, if included, the  $n^{\text{th}}$  occurrence of this  
3 field corresponds to the  $n^{\text{th}}$  occurrence of PilotPN in the record that  
4 contains the PilotPN field above.

5 Channel Channel record specification for the neighbor channel. See 10.1 for  
6 the Channel record format. The  $n^{\text{th}}$  occurrence of this field  
7 corresponds to the  $n^{\text{th}}$  occurrence of PilotPN in the record that  
8 contains the PilotPN field above.

9 SearchWindowSizeIncluded

10 The access network shall set this field to '1' if SearchWindowNeighbor  
11 field for neighboring sectors is included in this message. Otherwise,  
12 the access network shall set this field to '0'.

13 SearchWindowSize The access network shall omit this field if SearchWindowSizeIncluded  
14 is set to '0'. If SearchWindowSizeIncluded is set to '1', the access  
15 network shall set this field to the value shown in Table 6.6.6.5-1  
16 corresponding to the search window size to be used by the access  
17 terminal for the neighbor pilot. The  $n^{\text{th}}$  occurrence of this field  
18 corresponds to the  $n^{\text{th}}$  occurrence of PilotPN in the record that  
19 contains the PilotPN field above.

**Table 6.6.6.5-1. Search Window Sizes**

<b>SearchWindowSize Value</b>	<b>Search Window Size (PN chips)</b>
0	4
1	6
2	8
3	10
4	14
5	20
6	28
7	40
8	60
9	80
10	100
11	130
12	160
13	226
14	320
15	452

2    **SearchWindowOffsetIncluded**

3                 The access network shall set this field to '1' if SearchWindowOffset  
 4                 field for neighboring sectors is included in this message. Otherwise,  
 5                 the access network shall set this field to '0'.

6    **SearchWindowOffsetIncluded**

7                 The access network shall omit this field if  
 8                 SearchWindowOffsetIncluded is set to '0'. If  
 9                 SearchWindowOffsetIncluded is set to '1', the access network shall  
 10          set this field to the value shown in Table 6.6.6.5-2 corresponding to  
 11          the search window offset to be used by the access terminal for the  
 12          neighbor pilot. The  $n^{\text{th}}$  occurrence of this field corresponds to the  $n^{\text{th}}$   
 13          occurrence of PilotPN in the record that contains the PilotPN field  
 14          above.

**Table 6.6.6.5-2. Search Window Offset**

<b>SearchWindowOffset</b>	<b>Offset ( PN chips)</b>
0	0
1	$\text{WindowSize}^{28} / 2$
2	$\text{WindowSize}$
3	$3 \times \text{WindowSize} / 2$
4	$-\text{WindowSize} / 2$
5	$-\text{WindowSize}$
6	$-3 \times \text{WindowSize} / 2$
7	Reserved

2      Reserved      The number of bits in this field is equal to the number needed to  
 3      make the message length an integer number of octets. The access  
 4      network shall set this field to zero. The access terminal shall ignore  
 5      this field.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

## 6.6.6.5 Configuration Messages

8      The Default Route Update Protocol uses the Generic Configuration Protocol to transmit  
 9      configuration parameters from the access network to the access terminal. The following  
 10     messages are defined:

### 6.6.6.5.1 ConfigurationRequest

12     The access network sends the ConfigurationRequest message to override the defaults used  
 13     by the access terminal for a number of protocol parameters. The ConfigurationRequest  
 14     message format is given as part of the Generic Configuration Protocol (see 10.7).

15     The access network shall use a complex attribute (see 10.3) in the ConfigurationRequest  
 16     message.

17     The access network shall set the MessageID field of this message to 0x50.

18     The access network shall use the complex attributes defined in 6.6.6.5.1.1, 6.6.6.5.1.2, and  
 19     6.6.6.5.1.3 when sending the ConfigurationRequest message. If the access terminal does not  
 20     receive a ConfigurationRequest message, it shall use the following default values.

---

28    WindowSize is pilot's search window size in PN chips.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Best Effort
<b>Addressing</b>		unicast	<b>Priority</b>	60

1    6.6.6.5.1.1 SearchParameters Attribute  
2

<b>Field</b>	<b>Length (bits)</b>	<b>Default Value</b>
Length	8	N/A
AttributeID	8	N/A

3    One or more of the following record:  
4

ValueID	8	N/A
PilotIncrement	4	4
SearchWindowActive	4	8
SearchWindowNeighbor	4	10
SearchWindowRemaining	4	10

- 5    Length                         Length of the complex attribute in octets. The access network shall  
6    set this field to the length of the complex attribute excluding the  
7    Length field.
- 8    AttributeID                  The access network shall set this field to 0x00.
- 9    ValueID                         This field identifies this particular set of values for the attribute. The access network shall increment this field for each complex attribute-value record for a particular attribute.
- 10   PilotIncrement                 The access network shall set this field to the pilot PN sequence  
11   increment, in units of 64 PN chips, that access terminals are to use  
12   for searching the Remaining Set. The access network should set this  
13   field to the largest increment such that the pilot PN sequence offsets  
14   of all its neighbor access networks are integer multiples of that  
15   increment. The access terminal shall support all the valid values for  
16   this field.
- 17   SearchWindowActive             Search window size for the Active Set and Candidate Set. The access network shall set this field to the value shown in Table 6.6.6.5-1 corresponding to the search window size to be used by the access terminal for the Active Set and Candidate Set. The access terminal shall support all the valid values specified by this field.
- 18   SearchWindowNeighbor         Search window size for the Neighbor Set. The access network shall

1           set this field to the value shown in Table 6.6.6.5-1 corresponding to  
 2           the search window size to be used by the access terminal for the  
 3           Neighbor Set. The access terminal shall support all the valid values  
 4           specified by this field.

5           **SearchWindowRemaining**

6           Search window size for the Remaining Set. The access network shall  
 7           set this field to the value shown in Table 6.6.6.5-1 corresponding to  
 8           the search window size to be used by the access terminal for the  
 9           Remaining Set. The access terminal shall support all the valid values  
 10          specified by this field.

11         **6.6.6.5.1.2 SetManagementSameChannelParameters Attribute**

12         The access terminal shall use these attributes if the pilot being compared is on the same  
 13          channel as the active set pilots' channel.

<b>Field</b>	<b>Length (bits)</b>	<b>Default Value</b>
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PilotAdd	6	0x0e
PilotCompare	6	0x05
PilotDrop	6	0x12
PilotDropTimer	4	3
DynamicThresholds	1	0
SoftSlope	0 or 6	N/A
AddIntercept	0 or 6	N/A
DropIntercept	0 or 6	N/A
NeighborMaxAge	4	0
Reserved	variable	N/A

15         **Length**           Length of the complex attribute in octets. The access network shall  
 16           set this field to the length of the complex attribute excluding the  
 17           Length field.

18         **AttributeID**      The access network shall set this field to 0x01.

19         **ValueID**          This field identifies this particular set of values for the attribute. The  
 20           access network shall increment this field for each complex attribute-  
 21           value record for a particular attribute.

1	PilotAdd	This value is used by the access terminal to trigger a RouteUpdate in the Connected State. The access network shall set this field to the pilot detection threshold, expressed as an unsigned binary number equal to $\lfloor -2 \times 10 \times \log_{10} Ec/I_0 \rfloor$ . The value used by the access terminal is $-0.5$ dB times the value of this field. The access terminal shall support all the valid values specified by this field.
7	PilotDrop	This value is used by the access terminal to start a pilot drop timer for a pilot in the Active Set or the Candidate Set. The access network shall set this field to the pilot drop threshold, expressed as an unsigned binary number equal to $\lfloor -2 \times 10 \times \log_{10} Ec/I_0 \rfloor$ . The value used by the access terminal is $-0.5$ dB times the value of this field. The access terminal shall support all the valid values specified by this field.
14	PilotCompare	Active Set versus Candidate Set comparison threshold, expressed as a 2's complement number. The access terminal transmits a RouteUpdate message when the strength of a pilot in the Candidate Set exceeds that of a pilot in the Active Set by this margin. The access network shall set this field to the threshold Candidate Set pilot to Active Set pilot ratio, in units of $0.5$ dB. The access terminal shall support all the valid values specified by this field.
21	PilotDropTimer	Timer value after which an action is taken by the access terminal for a pilot that is a member of the Active Set or Candidate Set, and whose strength has not become greater than the value specified by PilotDrop. If the pilot is a member of the Active Set, a RouteUpdate message is sent in the Connected State. If the pilot is a member of the Candidate Set, it will be moved to the Neighbor Set. The access network shall set this field to the drop timer value shown in Table 6.6.6.5.1-1 corresponding to the pilot drop timer value to be used by access terminals. The access terminal shall support all the valid values specified by this field.

**Table 6.6.6.5.1-1. Pilot Drop Timer Values**

PilotDropTimer	Timer Expiration (seconds)	PilotDropTimer	Timer Expiration (seconds)
0	< 0.1	8	27
1	1	9	39
2	2	10	55
3	4	11	79
4	6	12	112
5	9	13	159
6	13	14	225
7	19	15	319

- |    |                   |  |
|----|-------------------|--|
| 2  | DynamicThresholds | This field shall be set to ‘1’ if the following three fields are included in this record. Otherwise, this field shall be set to ‘0’.   |
| 4  | SoftSlope         | This field shall be included only if DynamicThresholds is set to ‘1’. This field shall be set to an unsigned binary number, which is used by the access terminal in the inequality criterion for adding a pilot to the Active Set or dropping a pilot from the Active Set. The access terminal shall support all the valid values specified by this field. |
| 9  | AddIntercept      | This field shall be included only if DynamicThresholds is set to ‘1’. This field shall be set to a 2’s complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.   |
| 13 | DropIntercept     | This field shall be included only if DynamicThresholds is set to ‘1’. This field shall be set to a 2’s complement signed binary number in units of dB. The access terminal shall support all the valid values specified by this field.   |
| 17 | NeighborMaxAge    | The access network shall set this field to the maximum AGE value beyond which the access terminal is to drop members from the Neighbor Set. The access terminal shall support all the valid values specified by this field.  |
| 21 | Reserved          | The access network shall set this field to zero. The access terminal shall ignore this field. The length of this field shall be such that the entire record is octet-aligned.  |

## 1    6.6.6.5.1.3 SetManagementDifferentChannelParameters Attribute

2    The access terminal shall use these attributes if the pilot being compared is on a channel  
 3    that is different from the active set pilots' channel.

4

Field	Length (bits)	Default Value
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
PilotAdd	6	0x0e
PilotCompare	6	0x05
PilotDrop	6	0x12
PilotDropTimer	4	3
DynamicThresholds	1	0
SoftSlope	0 or 6	N/A
AddIntercept	0 or 6	N/A
DropIntercept	0 or 6	N/A
NeighborMaxAge	4	0
Reserved	variable	N/A

5    Length                 Length of the complex attribute in octets. The access network shall  
 6    set this field to the length of the complex attribute excluding the  
 7    Length field.

8    AttributeID          The access network shall set this field to 0x02.

9    ValueID              This field identifies this particular set of values for the attribute. The  
 10   access network shall increment this field for each complex attribute-  
 11   value record for a particular attribute.

12   PilotAdd             This value is used by the access terminal to trigger a RouteUpdate in  
 13   the Connected State. The access network shall set this field to the  
 14   pilot detection threshold, expressed as an unsigned binary number  
 15   equal to  $\lfloor -2 \times 10 \times \log_{10} Ec/I_0 \rfloor$ . The value used by the access  
 16   terminal is -0.5 dB times the value of this field. The access terminal  
 17   shall support all the valid values specified by this field.

18   PilotDrop            This value is used by the access terminal to start a pilot drop timer  
 19   for a pilot in the Active Set or the Candidate Set. The access network  
 20   shall set this field to the pilot drop threshold, expressed as an  
 21   unsigned binary number equal to  $\lfloor -2 \times 10 \times \log_{10} Ec/I_0 \rfloor$ . The value

1 used by the access terminal is  $-0.5$  dB times the value of this field.  
2 The access terminal shall support all the valid values specified by this  
3 field.

4 PilotCompare 5 Active Set versus Candidate Set comparison threshold, expressed as  
6 a 2's complement number. The access terminal transmits a  
7 RouteUpdate message when the strength of a pilot in the Candidate  
8 Set exceeds that of a pilot in the Active Set by this margin. The access  
9 network shall set this field to the threshold Candidate Set pilot to  
10 Active Set pilot ratio, in units of  $0.5$  dB. The access terminal shall  
support all the valid values specified by this field.

11 PilotDropTimer 12 Timer value after which an action is taken by the access terminal for  
13 a pilot that is a member of the Active Set or Candidate Set, and  
14 whose strength has not become greater than the value specified by  
15 PilotDrop. If the pilot is a member of the Active Set, a RouteUpdate  
16 message is sent in the Connected State. If the pilot is a member of  
17 the Candidate Set, it will be moved to the Neighbor Set. The access  
18 network shall set this field to the drop timer value shown in Table  
19 6.6.6.5.1-1 corresponding to the pilot drop timer value to be used by  
20 access terminals. The access terminal shall support all the valid  
values specified by this field.

21 DynamicThresholds 22 This field shall be set to '1' if the following three fields are included in  
this record. Otherwise, this field shall be set to '0'.

23 SoftSlope 24 This field shall be included only if DynamicThresholds is set to '1'.  
25 This field shall be set to an unsigned binary number, which is used  
26 by the access terminal in the inequality criterion for adding a pilot to  
the Active Set or dropping a pilot from the Active Set. The access  
27 terminal shall support all the valid values specified by this field.

28 AddIntercept 29 This field shall be included only if DynamicThresholds is set to '1'.  
30 This field shall be set to a 2's complement signed binary number in  
units of dB. The access terminal shall support all the valid values  
31 specified by this field.

32 DropIntercept 33 This field shall be included only if DynamicThresholds is set to '1'.  
34 This field shall be set to a 2's complement signed binary number in  
units of dB. The access terminal shall support all the valid values  
35 specified by this field.

36 NeighborMaxAge 37 The access network shall set this field to the maximum AGE value  
38 beyond which the access terminal is to drop members from the  
Neighbor Set. The access terminal shall support all the valid values  
39 specified by this field.

1    Reserved                          The access network shall set this field to zero. The access terminal  
 2                                        shall ignore this field. The length of this field shall be such that the  
 3                                        entire record is octet-aligned.

4    6.6.6.5.2 ConfigurationResponse

5    The access terminal sends the ConfigurationResponse message to select one of the complex  
 6                                        attributes offered by the access network. The ConfigurationResponse message format is  
 7                                        given as part of the Generic Configuration Protocol (see 10.7).

8    The access terminal shall set the MessageID field of this message to 0x51.

9    If the access terminal is sending an attribute with the message, the access terminal shall  
 10                                        set the ValueID field associated with this attribute to the ValueID field of the complex  
 11                                        attribute the access terminal is accepting.

<b>Channels</b>	AC	RTC	<b>SLP</b>	Best Effort
<b>Addressing</b>		unicast	<b>Priority</b>	60

13    6.6.7 Protocol Numeric Constants

Constant	Meaning	Value
N <sub>RUPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>RUPDefault</sub>	Subtype field for this protocol	0x0000
N <sub>RUPActive</sub>	Maximum size of the Active Set	6
N <sub>RUPCandidate</sub>	Maximum size of the Candidate Set	6
N <sub>RUPNeighbor</sub>	Minimum size of the Neighbor Set	20
T <sub>RUPPilotSupervision</sub>	Pilot supervision timer	10 seconds
T <sub>RUPConnectionSetup</sub>	Maximum time to receive an indication at the AT that the connection is set up from the instant it receives a TrafficChannelAssignment message.	1 second

15    6.6.8 Interface to Other Protocols

16    6.6.8.1 Commands Sent

17    This protocol sends the following commands:

- 18      • *ReverseTrafficChannelMAC.Activate*
- 19      • *ReverseTrafficChannelMAC.Deactivate*
- 20      • *ForwardTrafficChannelMAC.Activate*
- 21      • *ForwardTrafficChannelMAC.Deactivate*

1    6.6.8.2 Indications

2    This protocol registers to receive the following indications:

- 3       • *ReverseTrafficChannelMAC.LinkAcquired*

- 4       • *OverheadMessages.Updated*

5

**6.7 Default Packet Consolidation Protocol**

## 6.7.1 Overview

The Default Packet Consolidation Protocol provides packet consolidation on the transmit side and provides packet de-multiplexing on the receive side. Packet consolidation is provided between different streams at the access terminal and between different streams associated with one access terminal, as well as between different access terminals at the access network.

## 6.7.2 Primitives and Public Data

## 6.7.2.1 Commands

This protocol does not define any commands.

## 6.7.2.2 Return Indications

This protocol does not return any indications.

## 6.7.2.3 Public Data

- None

## 6.7.3 Basic Protocol Numbers

The Type field for the Packet Consolidation Protocol is one octet, set to  $N_{PCPType}$ .

The Subtype field for the Default Packet Consolidation Protocol is two octets, set to  $N_{PCPDefault}$ .

## 6.7.4 Protocol Data Unit

The Protocol Data Unit for this protocol is a Connection Layer packet. Connection Layer packets contain Session Layer packets destined to or from the same access terminal address.

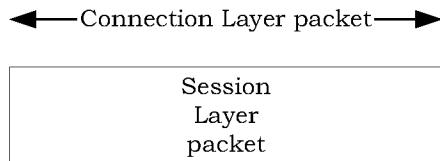
Two types of Connection Layer packets are defined:

- Format A: These packets are maximum length packets (including lower layer headers). Format A packets contain one Session Layer packet and do not have Connection Layer headers or padding.
- Format B: These packets are maximum length packets (including lower layer headers). Format B packets contain one or more Session Layer packets and have a Connection Layer header(s). The protocol places the Connection Layer header defined in 6.7.6.2 in front of each Session Layer packet and enough padding to create a maximum length packet.

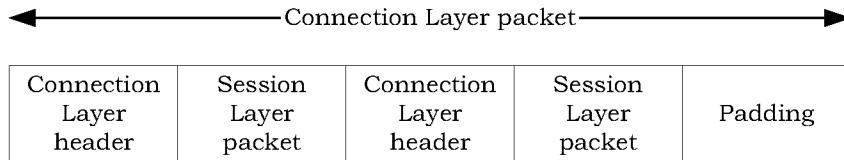
Format A provides an extra byte of payload per packet.

The packet format type is passed with the packet to the lower layers.

- 1 The Connection Layer encapsulation is shown in Figure 6.7.4-1 and Figure 6.7.4-2.
- 2 All transmitted packets are forwarded to the Security Layer.
- 3 All received packets are forwarded to the Session Layer after removing the Connection Layer headers.
- 4
- 5 The maximum size Session Layer packet the protocol can encapsulate depends on the
- 6 Physical Layer channel on which this packet will be transmitted and on the specific security
- 7 protocols negotiated.



**Figure 6.7.4-1. Connection Layer Packet Structure (Format A)**



**Figure 6.7.4-2. Connection Layer Packet Structure (Format B)**

### 6.7.5 Procedures

This protocol does not have any initial configuration requirements.

This protocol receives the following information with every transmitted Session Layer packet:

- Destination channel: Forward Traffic Channel, Control Channel, Reverse Traffic Channel, or Access Channel.
- Priority.
- Forced Single Encapsulation: Whether or not the Session Layer packet can be encapsulated with other Session Layer packets in the same Connection Layer packet.

#### 6.7.5.1 Destination Channels

If the destination channel is the Forward Traffic Channel, the packet also carries a parameter indicating whether the protocol is allowed to transmit it in a Control Channel capsule.

If the destination channel is the Control Channel, the packet also carries a parameter indicating whether the packet must be transmitted in a synchronous capsule. If the packet

1 does not have to be transmitted in a synchronous capsule, it may carry a parameter  
2 indicating a transmission deadline.

3 **6.7.5.2 Priority Order**

4 Packets are prioritized according to the following rules:

- 5     • If two packets have different priority numbers, the packet with the lower priority  
6       number has priority.  
7     • If two packets have the same priority number, the packet that was received first by  
8       the protocol has priority.

9 Transmission of packets that have higher priority shall take precedence over transmission  
10 of packets with lower priority.

11 Processing packets that have higher priority shall take precedence over processing packets  
12 with lower priority.

13 **6.7.5.3 Forced Single Encapsulation**

14 If a Forward Traffic Channel Session Layer packet is marked as Forced Single  
15 Encapsulation, the access network shall encapsulate it without any other Session Layer  
16 packets in a Connection Layer packet. The Packet Consolidation Protocol shall also pass an  
17 indication down to the physical layer with the Connection Layer packet, instructing the  
18 physical layer to ensure that the Physical Layer packet containing this packet does not  
19 contain any other Connection Layer packet. Forced Single Encapsulation applies only to the  
20 Forward Traffic Channel MAC Layer packets.

21 Forced Single Encapsulation is used for test services that require a one to one mapping  
22 between application packets and Physical Layer packets.

23 **6.7.5.4 Access Terminal Procedures**

24 **6.7.5.4.1 Format A Packets**

25 The access terminal shall create a Format A Connection Layer packet, only if the highest  
26 priority pending Session Layer packet will fill the Security Layer payload.

27 The access terminal shall forward the Connection Layer packet for transmission to the  
28 Security Layer.

29 **6.7.5.4.2 Format B Packets**

30 The access terminal shall create a Format B Connection Layer packet by adding the  
31 Connection Layer header, defined in 6.7.6.2 in front of every Session Layer packet,  
32 concatenating the result and adding enough padding to fill the Security Layer payload. The  
33 resulting packet length shall not exceed the maximum payload that can be carried on the  
34 Physical Layer Channel, given the transmission rate that will be used to transmit the

1 packet and the headers added by the lower layers. All concatenated Connection Layer  
2 packets shall be transmitted on the same Physical Layer Channel.<sup>29</sup>

3 The protocol shall encapsulate and concatenate Session Layer packets in priority order.  
4 The access terminal shall forward the Connection Layer packet for transmission to the  
5 Security Layer.

6 6.7.5.5 Access Network Procedures

7 6.7.5.5.1 Control Channel

8 The Control Channel carries broadcast transmissions as well as directed transmissions to  
9 multiple access terminals.

10 If the access network transmits a unicast packet to an access terminal over the Control  
11 Channel, it should transmit this packet at least from all the sectors in the access terminal's  
12 Active Set. If the data is carried in a synchronous capsule, the transmission should occur  
13 simultaneously at least once.

14 The access network shall create the Connection Layer packets as defined in 6.7.5.5.1.1.

15 The access network shall prioritize Connection Layer packets marked for transmission in a  
16 Control Channel synchronous capsule as defined in 6.7.5.5.1.2.

17 The access network shall prioritize Connection Layer packets marked for transmission in a  
18 Control Channel asynchronous capsule as defined in 6.7.5.5.1.1 and 6.7.5.5.1.3

19 6.7.5.5.1.1 Control Channel Connection Layer Packets

20 The access network shall not encapsulate Session Layer packets destined to different access  
21 terminals in the same Connection Layer packet.

22 The access network may encapsulate multiple Session Layer packets destined to a single  
23 access terminal in the same Connection Layer packet.

24 The access network should assign a priority to the Connection Layer packet based on its  
25 component Session Layer packets. If the Connection Layer packet contains a single Session  
26 Layer packet, the priority of the Connection Layer packet should be the priority received  
27 with the Session Layer packet.

28 If any Session Layer packet encapsulated in a Connection Layer packet is marked for  
29 transmission in a synchronous capsule, the Connection Layer packet shall be marked for  
30 transmission in a synchronous capsule.

31 The access network shall create a Connection Layer packet by appending the Connection  
32 Layer header defined in 6.7.6.2 in front of every Session Layer packet it is encapsulating in  
33 this Connection Layer packet and then concatenating the result. The resulting packet  
34 length shall not exceed the maximum payload that can be carried in a Control Channel  
35 MAC Layer packet given the headers added by the lower layers.

---

<sup>29</sup> i.e., Access Channel or Reverse Traffic Channel.

1 The access network shall forward the Connection Layer packet for transmission to the  
2 Security Layer.

3 6.7.5.5.1.2 Synchronous Capsule Priority Rules

4 The access network should transmit, in priority order, all Connection Layer packets marked  
5 for transmission in a Control Channel synchronous capsule. If the amount of transmitted  
6 data (including lower layer headers) exceeds a single Control Channel MAC Layer packet,  
7 the access network may extend the synchronous capsule, delay the transmission of some  
8 Session Layer packets, or discard Session Layer packets. If the access network discards  
9 packets, it should discard them in reverse priority order.

10 In addition to transmitting the above Connection Layer packets, the access network may  
11 also transmit the following packets in a synchronous Control Channel capsule:

- 12 • Packets marked for transmission in an asynchronous Control Channel capsule, in  
13 priority order
- 14 • Packets marked for transmission either on the Forward Traffic Channel or the  
15 Control Channel, in priority order

16 If the access network transmits these additional packets, it should follow the above priority  
17 ordering, and should transmit them at a lower priority than packets marked for  
18 transmission in synchronous capsules only.

19 6.7.5.5.1.3 Asynchronous Capsule Priority Rules

20 Transmitting asynchronous capsules on the Control Channel is optional, because all data  
21 marked for transmission in these capsules can also be transmitted in a synchronous  
22 capsule.

23 If the access network chooses to transmit Connection Layer packets in an asynchronous  
24 capsule of the Control Channel, it should do so in the following order:

- 25 • Packets marked for transmission in an asynchronous capsule of the Control  
26 Channel, in priority order
- 27 • Packets marked for transmission either on the Forward Traffic Channel or the  
28 Control Channel, in priority order

29 6.7.5.5.2 Forward Traffic Channel

30 The Forward Traffic Channel is time-multiplexed between the different access terminals.  
31 The transmission priority given to each access terminal is beyond the scope of this  
32 specification.<sup>30</sup>

---

<sup>30</sup> Typical considerations for the access network are throughput maximization balanced with a fairness criteria between users.

## 1    6.7.5.5.2.1 Format A Packets

2    The access network shall create a Format A Connection Layer packet, only if the length of  
 3    the highest priority pending Session Layer packet will fill the security layer payload.

4    The access network shall forward the Connection Layer packet for transmission to the  
 5    Security Layer.

## 6    6.7.5.5.2.2 Format B Packets

7    The access network shall create a Format B Connection Layer packet by adding the  
 8    Connection Layer header defined in 6.7.6.2 in front of every Session Layer packet,  
 9    concatenating the result and adding padding to fill the Security Layer payload. The  
 10   resulting packet length shall not exceed the maximum payload that can be carried on the  
 11   Forward Traffic Channel given the headers added by the lower layers.

12   The protocol shall encapsulate and concatenate Session Layer packets in priority order.

13   The access network shall forward the Connection Layer packet for transmission to the  
 14   Security Layer.

## 15   6.7.6 Header Format

## 16   6.7.6.1 Pad

17   The access network shall add sufficient padding so that the packet fills the Security Layer  
 18   payload.

19   The access network shall set the padding bits to '0'. The access terminal shall ignore the  
 20   padding bits.

## 21   6.7.6.2 Connection Layer Header

22   The access terminal and the access network add the following header in front of every  
 23   Session Layer packet encapsulated in a Format B Connection Layer packet.

<b>Field</b>	<b>Length (bits)</b>
Length	8

25   Length                          Length of Session Layer packet in octets.

## 26   6.7.7 Protocol Numeric Constants

27

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>PCPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>PCPDefault</sub>	Subtype field for this protocol	0x0000

- 1    6.7.8 Interface to Other Protocols
- 2    6.7.8.1 Commands Sent
- 3    This protocol does not issue any commands.
- 4    6.7.8.2 Indications
- 5    This protocol does not register to receive any indications.
- 6

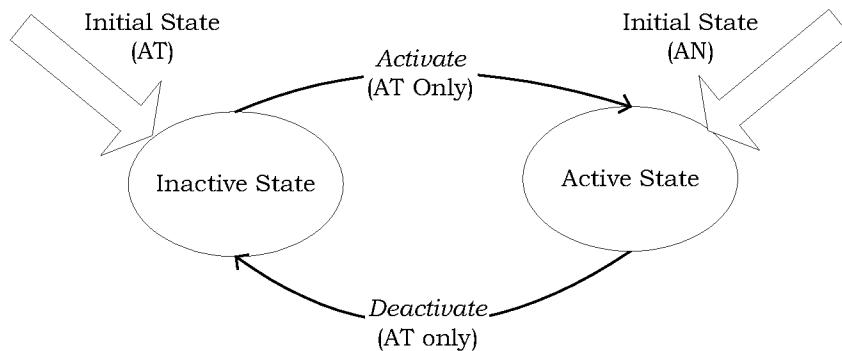
## 1   **6.8 Overhead Messages Protocol**

### 2   6.8.1 Overview

3   The QuickConfig message and the SectorParameters message are collectively termed the  
 4   overhead messages. These messages are broadcast by the access network over the Control  
 5   Channel. These messages are unique, in that they pertain to multiple protocols and are,  
 6   therefore, specified separately. The Overhead Messages Protocol provides procedures related  
 7   to transmission, reception and supervision of these messages.

8   This protocol can be in one of two states:

- 9   • Inactive State: In this state, the protocol waits for an *Activate* command. This state  
 10   corresponds only to the access terminal and occurs when the access terminal has not  
 11   acquired an access network or is not required to receive overhead messages.
- 12   • Active State: In this state the access network transmits and the access terminal  
 13   receives overhead messages.



15   **Figure 6.8.1-1. Overhead Messages Protocol State Diagram**

### 16   6.8.2 Primitives and Public Data

#### 17   6.8.2.1 Commands

18   This protocol defines the following commands:

- 19   • *Activate*
- 20   • *Deactivate*

#### 21   6.8.2.2 Return Indications

22   This protocol returns the following indications:

- 23   • *ANRedirected*
- 24   • *SupervisionFailed*
- 25   • *Updated*

1    6.8.2.3 Public Data

2    This protocol shall make the following data public:

- 3       • all data in the overhead messages  
4       • OverheadParametersUpToDate

5    6.8.3 Basic Protocol Numbers

6    The Type field for the Overhead Messages is one octet, set to  $N_{OMPType}$ .

7    The Subtype field for this protocol is two octets set to  $N_{OMPDefault}$ .<sup>31</sup>

8    6.8.4 Protocol Data Unit

9    The transmission unit of this protocol is a message. This is a control protocol; and,  
10 therefore, it does not carry payload on behalf of other layers or protocols.

11    This protocol uses the Signaling Application to transmit and receive messages.

12    6.8.5 Procedures

13    6.8.5.1 Protocol Initialization and Configuration

14    The access terminal shall start this protocol in the Inactive State.

15    The access network shall start this protocol in the Active State.

16    This protocol does not have any initial configuration requirements.

17    6.8.5.2 Extensibility Requirements

18    Further revisions of the access network may add new overhead messages.

19    The access terminal shall discard overhead messages with a MessageID field it does not  
20 recognize.

21    Further revisions of the access network may add new fields to existing overhead messages.  
22    These fields shall be added to the end of the message, prior to the Reserved field if such a  
23 field is defined.

24    The access terminal shall ignore fields it does not recognize.

25    6.8.5.3 Command Processing

26    The access network shall ignore all commands.

27    6.8.5.3.1 Activate

28    If this protocol receives an *Activate* command in the Inactive State:

- 29       • The access terminal shall transition to the Active State.

---

<sup>31</sup> This protocol is not negotiable; and, therefore, the protocol Subtype is currently not used.

- 1        • The access network shall ignore it.  
 2        If this protocol receives the command in the Active State, it shall be ignored.

3        6.8.5.3.2 Deactivate

- 4        If this protocol receives a *Deactivate* command in the Inactive State, it shall be ignored.  
 5        If this protocol receives the command in the Active State:

- 6        • Access terminal shall transition to the Inactive State.
- 7        • Access network shall ignore it.

8        6.8.5.4 Access Network Requirements

9        The access network shall include a QuickConfig message in every Control Channel  
 10      synchronous capsule. The access network should include a SectorParameters message in  
        the synchronous capsule at least once every  $N_{OMPSectorParameters}$  Control Channel cycles. The  
 12      access network shall set the SectorSignature field of the QuickConfig message to the  
 13      SectorSignature field of the next SectorParameters message. The access network shall set  
 14      the AccessSignature field of the QuickConfig message to the public data AccessSignature  
 15      (see Default Access Channel MAC Protocol).

16      6.8.5.5 Access Terminal Requirements

17      When the access terminal is required to keep the overhead messages updated, it shall  
 18      perform supervision on the QuickConfig and the SectorParameters messages as specified in  
 19      6.8.5.5.1.1 and 6.8.5.5.1.2, respectively.

20      If the access terminal does not have any stored value for the overhead parameters or if it  
 21      receives a *RouteUpdate.IdleHO* indication, the access terminal shall set  
 22      OverheadParametersUpToDate to 0.

23      When the access terminal receives the QuickConfig message, it shall perform the following:

- 24        • If the value of the SectorSignature field of the new QuickConfig message is different  
             from the stored value for SectorSignature, the access terminal shall perform the  
             following:

- 27        – The access terminal shall set OverheadParametersUpToDate to 0.
- 28        – The access terminal shall monitor every subsequent Control Channel synchronous  
             capsule until it receives the updated SectorParameters message. When the access  
             terminal receives the updated SectorParameters message, it shall return an  
             *Updated* indication and set OverheadParametersUpToDate to 1.

- 32        • Otherwise, the access terminal shall perform the following:

- 33        – The access terminal shall set OverheadParametersUpToDate to 1.
- 34        – The access terminal shall return an *Updated* indication.

35      Once the access terminal receives an updated overhead message, it should store the  
 36      signature associated with the message for future comparisons. The access terminal may

cache overhead message parameters and signatures to speed up acquisition of parameters from a sector that was previously monitored.

If the Redirect field of the QuickConfig message is set to '1', the access terminal shall return an *ANRedirected* indication.<sup>32</sup>

##### 6.8.5.5.1 Supervision Procedures

###### 6.8.5.5.1.1 Supervision of QuickConfig Message

Upon entering the Active State, the access terminal shall start the following procedure to supervise the QuickConfig message:

- The access terminal shall set a QuickConfig supervision timer for  $T_{OMPQCSupervision}$ .
- If a QuickConfig message is received while the timer is active, the access terminal shall reset and restart the timer.
- If the timer expires, the access terminal shall return a *SupervisionFailed* indication and disable the timer.

###### 6.8.5.5.1.2 Supervision of SectorParameters Message

Upon entering the Active State, the access terminal shall start the following procedure to supervise the SectorParameters message:

- The access terminal shall set a SectorParameters supervision timer for  $T_{OMPSPSupervision}$ .
- If a SectorParameters message is received while the timer is active, the access terminal shall reset and restart the timer.
- If the timer expires, the access terminal shall return a *SupervisionFailed* indication and disable the timer.

##### 6.8.6 Message Formats

###### 6.8.6.1 QuickConfig

The QuickConfig message is used to indicate a change in the overhead messages' contents and to provide frequently changing information.

---

<sup>32</sup> Redirection is commonly used in networks under test.

Field	Length (bits)
MessageID	8
ColorCode	8
SectorID24	24
SectorSignature	16
AccessSignature	16
Redirect	1
RPCCount	6

RPCCount occurrences of the following field

DRClock	1
---------	---

RPCCount occurrences of the following field

ForwardTrafficValid	1
---------------------	---

Reserved variable

- |    |                 |   |
|----|-----------------|---|
| 1  | MessageID       | The access network shall set this field to 0x00.  |
| 2  | ColorCode       | The access network shall set this field to the color code corresponding to this sector.   |
| 3  | SectorID24      | The access network shall set this field to the least significant 24 bits of the SectorID value corresponding to this sector.  |
| 4  | SectorSignature | The access network shall set this field to the value of the SectorSignature field of the next SectorParameters message it will transmit.  |
| 5  | AccessSignature | The access network shall set this field to the value of the AccessSignature parameter from the AccessParameters message that is Public Data of the Access Channel MAC Protocol. |
| 6  | Redirect        | Access network redirect. The access network shall set this field to '1' if it is redirecting all access terminals away from this access network. <sup>33</sup>                  |
| 7  | RPCCount        | The access network shall set this field to the maximum number of RPC channels supported by the sector.  |
| 8  |                 |   |
| 9  |                 |   |
| 10 |                 |   |
| 11 |                 |   |
| 12 |                 |   |
| 13 |                 |   |
| 14 |                 |   |
| 15 |                 |   |
| 16 |                 |   |

<sup>33</sup> Network redirect is commonly used during testing.

- 1      DRClock                The access network shall set occurrence  $n$  of this field to ‘1’ if it has  
 2                                  received a valid DRC from the access terminal that has been assigned  
 3                                  MACIndex 64- $n$  (e.g., occurrence 1 of this field, corresponds to  
 4                                  MACIndex 63).
- 5      ForwardTrafficValid    The access network shall set occurrence  $n$  of this field to ‘1’ if the  
 6                                  Forward Traffic Channel associated with MACIndex 64- $n$  is valid. The  
 7                                  access terminal uses this field to perform supervision of the Forward  
 8                                  Traffic Channel.
- 9      Reserved                The number of bits in this field is equal to the number needed to  
 10                                 make the message length an integer number of octets. The access  
 11                                 network shall set this field to zero. The access terminal shall ignore  
 12                                 this field.
- 13

<b>Channels</b>	CCsyn	<b>SLP</b>	Best Effort
<b>Addressing</b>	broadcast	<b>Priority</b>	10

#### 14      6.8.6.2 SectorParameters

15      The SectorParameters message is used to convey sector specific information to the access  
 16                                 terminals.

17

Field	Length (bits)
MessageID	8
SectorID	128
SubnetMask	8
SectorSignature	16
Latitude	22
Longitude	23
RouteUpdateRadius	11
LeapSeconds	8
LocalTimeOffset	11
ChannelCount	5

ChannelCount occurrences of the following field:

Channel	24
---------	----

NeighborCount	5
---------------	---

NeighborCount occurrences of the following field:

NeighborPilotPN	9
-----------------	---

NeighborCount occurrences of the following two fields:

NeighborChannelIncluded	1
NeighborChannel	0 or 24

NeighborSearchWindowSizeIncluded	1
----------------------------------	---

NeighborCount occurrences of the following field

NeighborSearchWindowSize	0 or 4
--------------------------	--------

NeighborSearchWindowOffsetIncluded	1
------------------------------------	---

NeighborCount occurrences of the following field

NeighborSearchWindowOffset	0 or 3
----------------------------	--------

Reserved	Variable
----------	----------

<sup>1</sup> MessageID      The access network shall set this field to 0x01.

<sup>2</sup> SectorID      Sector Address Identifier. The access network shall set this field to the 128-bit address of this sector.

1	SubnetMask	Sector Subnet identifier. The access network shall set this field to the number of consecutive 1's in the subnet mask of the subnet to which this sector belongs.
4	SectorSignature	SectorParameters message signature. The access network shall change this field if the contents of the SectorParameters message changes.
7	Latitude	The latitude of the sector. The access network shall set this field to this sector's latitude in units of 0.25 second, expressed as a two's complement signed number with positive numbers signifying North latitudes. The access network shall set this field to a value in the range -1296000 to 1296000 inclusive (corresponding to a range of -90° to +90°).
13	Longitude	The longitude of the sector. The access network shall set this field to this sector's longitude in units of 0.25 second, expressed as a two's complement signed number with positive numbers signifying East longitude. The access network shall set this field to a value in the range -2592000 to 2592000 inclusive (corresponding to a range of -180° to +180°).
19	RouteUpdateRadius	If access terminals are to perform distance based route updates, the access network shall set this field to the non-zero "distance" beyond which the access terminal is to send a new RouteUpdate message (see Default Route Update Protocol). If access terminals are not to perform distance based route updates, the access network shall set this field to 0. <sup>34</sup>
25	LeapSeconds	The number of leap seconds that have occurred since the start of system time.
27	LocalTimeOffset	The access network shall set this field to the offset of the local time from System Time. This value will be in units of minutes, expressed as a two's complement signed number.
30	ChannelCount	The access network shall set this field to the number of cdma2000 high rate packet data channels available to the access terminal on this sector.

---

<sup>34</sup> The access terminal determines whether to send a distance based RouteUpdate message or not using the RouteUpdateRadius value of the serving sector. If the serving sector allows distance based Route Updates, the access terminal uses the RouteUpdateRadius value sent by the sector in which the access terminal last registered.

- |    |                                  |   |
|----|----------------------------------|---|
| 1  | Channel                          | Channel record specification for each channel. See 10.1 for the Channel record format. The access network shall set the SystemType field of this record to 0x00.  |
| 2  |                                  |   |
| 3  |                                  |   |
| 4  | NeighborCount                    | The access network shall set this field to the number of records specifying neighboring sectors information included in this message.   |
| 5  |                                  |   |
| 6  | NeighborPilotPN                  | The access network shall set this field to the PN Offset of a neighboring sector that the access terminal should add to its Neighbor Set.   |
| 7  |                                  |   |
| 8  |                                  |   |
| 9  | NeighborChannelIncluded          | The access network shall set this field to '1' if a Channel record is included for this neighbor, and to '0' otherwise. The $n^{\text{th}}$ occurrence of this field corresponds to the $n^{\text{th}}$ occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.  |
| 10 |                                  |   |
| 11 |                                  |   |
| 12 |                                  |   |
| 13 |                                  |   |
| 14 | NeighborChannel                  | Channel record specification for the neighbor channel. See 10.1 for the Channel record format. The access network shall omit this field if the corresponding NeighborChannelIncluded field is set to '0'. Otherwise, if included, the $n^{\text{th}}$ occurrence of this field corresponds to the $n^{\text{th}}$ occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above.  |
| 15 |                                  |   |
| 16 |                                  |   |
| 17 |                                  |   |
| 18 |                                  |   |
| 19 |                                  |   |
| 20 | NeighborSearchWindowSizeIncluded | The access network shall set this field to '1' if NeighborSearchWindowSize field for neighboring sectors is included in this message. Otherwise, the access network shall set this field to '0'.  |
| 21 |                                  |   |
| 22 |                                  |   |
| 23 |                                  |   |
| 24 | NeighborSearchWindowSize         | The access network shall omit this field if NeighborSearchWindowSizeIncluded is set to '0'. If NeighborSearchWindowSizeIncluded is set to '1', the access network shall set this field to the value shown in Table 6.8.6.2-1 corresponding to the search window size to be used by the access terminal for the neighbor pilot. The $n^{\text{th}}$ occurrence of this field corresponds to the $n^{\text{th}}$ occurrence of NeighborPilotPN in the record that contains the NeighborPilotPN field above. |
| 25 |                                  |   |
| 26 |                                  |   |
| 27 |                                  |   |
| 28 |                                  |   |
| 29 |                                  |   |
| 30 |                                  |   |
| 31 |                                  |   |
| 32 |                                  |   |

**Table 6.8.6.2-1. Search Window Sizes**

<b>SearchWindowSize Value</b>	<b>Search Window Size (PN chips)</b>
0	4
1	6
2	8
3	10
4	14
5	20
6	28
7	40
8	60
9	80
10	100
11	130
12	160
13	226
14	320
15	452

## 2 NeighborSearchWindowOffsetIncluded

3                         The access network shall set this field to '1' if  
 4                         NeighborSeachWindowOffset field for neighboring sectors is included  
 5                         in this message. Otherwise, the access network shall set this field to  
 6                         '0'.

## 7 NeighborSeachWindowOffset

8                         The access network shall omit this field if  
 9                         NeighborSearchWindowOffsetIncluded is set to '0'. If  
 10                         NeighborSearchWindowOffsetIncluded is set to '1', the access network  
 11                         shall set this field to the value shown in Table 6.8.6.2-2  
 12                         corresponding to the search window offset to be used by the access  
 13                         terminal for the neighbor pilot. The  $n^{\text{th}}$  occurrence of this field  
 14                         corresponds to the  $n^{\text{th}}$  occurrence of NeighborPilotPN in the record  
 15                         that contains the NeighborPilotPN field above.

**Table 6.8.6.2-2. Search Window Offset**

<b>SearchWindowOffset</b>	<b>Offset ( PN chips)</b>
0	0
1	WindowSize <sup>35</sup> /2
2	WindowSize
3	3 × WindowSize /2
4	- WindowSize /2
5	- WindowSize
6	-3 × WindowSize /2
7	Reserved

2 Reserved The number of bits in this field is equal to the number needed to make the  
 3 message length an integer number of octets. The access network shall set this field to zero.  
 4 The access terminal shall ignore this field.

<b>Channels</b>	CC	<b>SLP</b>	Best Effort
<b>Addressing</b>	broadcast	<b>Priority</b>	30

## 6.8.7 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
NOMPType	Type field for this protocol	Table 2.3.6-1
NOMPDefault	Subtype field for this protocol	0x0000
TOMPQCSupervision	QuickConfig supervision timer	12 Control Channel cycles
TOMPSPSupervision	SectorParameters supervision timer	12 Control Channel cycles
NOMPSectorParameters	The recommended maximum number of Control Channel cycles between two consecutive SectorParameters message transmissions	3

## 6.8.8 Interface to Other Protocols

### 6.8.8.1 Commands Sent

This protocol does not send any commands.

---

<sup>35</sup> WindowSize is pilot's search window size in PN chips.

1        6.8.8.2 Indications

2        This protocol registers to receive the following indication:

- 3              • *RouteUpdate.IdleHO*

4

- 1 No text.

**7 SECURITY LAYER****7.1 Introduction**

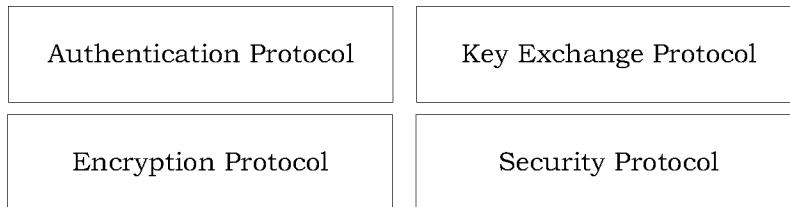
## 7.1.1 General Overview

The Security Layer provides the following functions:

- Key Exchange: Provides the procedures followed by the access network and by the access terminal to exchange security keys for authentication and encryption.
- Authentication: Provides the procedures followed by the access network and the access terminal for authenticating traffic.
- Encryption: Provides the procedures followed by the access network and the access terminal for encrypting traffic.

The Security Layer uses the Key Exchange Protocol, Authentication Protocol, Encryption Protocol, and Security Protocol to provide these functions. Security Protocol provides public variables needed by the authentication and encryption protocols (e.g., cryptosync, timestamp, etc.).

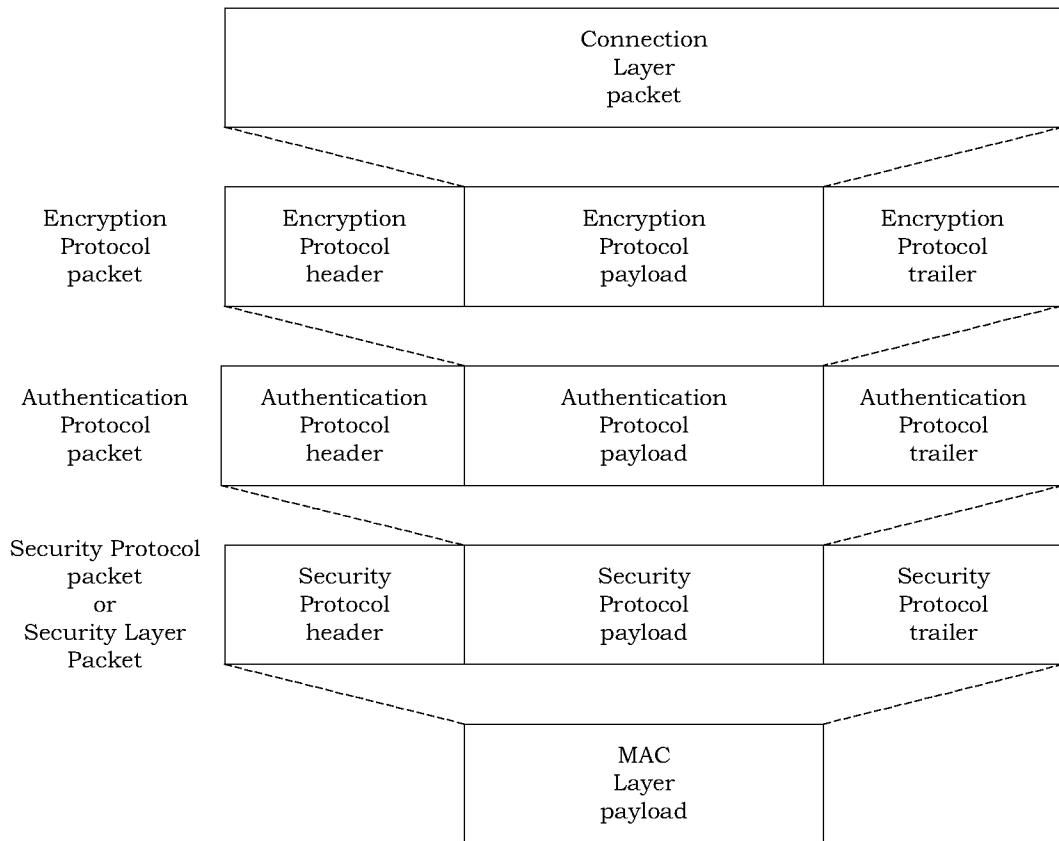
Figure 7.1.1-1 shows the protocols within the Security Layer.



**Figure 7.1.1-1. Security Layer Protocols**

**7.2 Data Encapsulation**

Figure 7.2-1 illustrates the relationship between a Connection Layer packet, a Security Layer packet and a MAC Layer payload.



**Figure 7.2-1. Security Layer Encapsulation**

The Security Layer headers or trailers may not be present (or equivalently, have a size of zero) if session configuration establishes the Default Security Layer or if the configured Security Protocol does not require a header or trailer. The fields added by the MAC Layer indicate presence (or absence) of the Security Layer headers and trailers. The Encryption Protocol may add a trailer to hide the actual length of the plain-text or padding to be used by the encryption algorithm. The Encryption Protocol Header may contain variables such as initialization vector (IV) to be used by the Encryption Protocol. The Authentication Protocol header or trailer may contain the digital signature that is used to authenticate the portion of the Authentication Protocol Packet that is authenticated. The Security Protocol header or trailer may contain variables needed by the authentication and encryption protocols (e.g., cryptosync, time-stamp, etc.).

Figure 7.2-1 shows the portions of the security layer packet that may be encrypted and authenticated. The authentication is performed on the Encryption Protocol Packet. This avoids unnecessary decryption when authentication fails.

The Security Layer shall pass the ConnectionLayerFormat field given to it by the MAC Layer to the Connection Layer with the Connection Layer packet.

1    7.2.1 Primitives and Public Data

2    7.2.1.1 Key Exchange Protocol

3    7.2.1.1.1 Commands

4    This protocol does not define any commands.

5    7.2.1.1.2 Return Indications

6    This protocol does not return any indication.

7    7.2.1.1.3 Public Data

- 8    • FACAuthKey

9         The authentication key for use on Forward Assigned Channels (e.g., the Forward  
10      Traffic Channel).

- 11    • RACAuthKey

12         The authentication key for use on Reverse Assigned Channels (e.g., the Reverse  
13      Traffic Channel).

- 14    • FACEncKey

15         The encryption key for use on Forward Assigned Channels (e.g., the Forward Traffic  
16      Channel).

- 17    • RACEncKey

18         The encryption key for use on Reverse Assigned Channels (e.g., the Reverse Traffic  
19      Channel).

- 20    • FPCAuthKey

21         The authentication key for use on Forward Public Channels (e.g., the Control  
22      Channel).

- 23    • RPCAuthKey

24         The authentication key for use on Reverse Public Channels (e.g., the Access  
25      Channel).

- 26    • FPCEncKey

27         The encryption key for use on Forward Public Channels (e.g. the Control Channel).

- 28    • RPCEncKey

29         The encryption key for use on Reverse Public Channels (e.g. the Access Channel).

30    7.2.1.1.4 Basic Protocol Numbers

31    The Type field for this protocol is one octet, set to N<sub>KEPType</sub>.

32    7.2.1.1.5 Interface to Other Protocols

33    7.2.1.1.5.1 Commands

34    This protocol does not define any commands.

- 1    7.2.1.1.5.2 Indications
- 2    This protocol does not register to receive any indications.
- 3    7.2.1.2 Encryption Protocol
- 4    7.2.1.2.1 Commands
- 5    This protocol does not define any commands.
- 6    7.2.1.2.2 Return Indications
- 7    This protocol returns the following indication:
  - 8       • *Failed*
- 9    7.2.1.2.3 Public Data
- 10    This protocol does not define any public data.
- 11    7.2.1.2.4 Basic Protocol Numbers
- 12    The Type field for this protocol is one octet, set to  $N_{EPTtype}$ .
- 13    7.2.1.2.5 Interface to Other Protocols
- 14    7.2.1.2.5.1 Commands
- 15    This protocol does not issue any commands.
- 16    7.2.1.2.5.2 Indications
- 17    This protocol does not register to receive any indications.
- 18    7.2.1.3 Authentication Protocol
- 19    7.2.1.3.1 Commands
- 20    This protocol does not define any commands.
- 21    7.2.1.3.2 Return Indications
- 22    This protocol returns the following indication:
  - 23       • *Failed*
- 24    7.2.1.3.3 Public Data
- 25    This protocol does not define any public data.
- 26    7.2.1.3.4 Basic Protocol Numbers
- 27    The Type field for this protocol is one octet, set to  $N_{APType}$ .

- 1      7.2.1.3.5 Interface to Other Protocols
- 2      7.2.1.3.5.1 Commands
- 3      This protocol does not issue any commands.
- 4      7.2.1.3.5.2 Indications
- 5      This protocol does not register to receive any indications.
- 6      7.2.1.4 Security Protocol
- 7      7.2.1.4.1 Commands
- 8      This protocol does not define any commands.
- 9      7.2.1.4.2 Return Indications
- 10     This protocol does not return any indications.
- 11     7.2.1.4.3 Public Data
  - 12       • TimeStampLong
- 13     7.2.1.4.4 Basic Protocol Numbers
- 14     The Type field for this protocol is one octet, set to N<sub>SPType</sub>.
- 15     7.2.1.4.5 Interface to Other Protocols
- 16     7.2.1.4.5.1 Commands
- 17     This protocol does not issue any commands.
- 18     7.2.1.4.5.2 Indications
- 19     This protocol does not register to receive any indications.
- 20

1   **7.3 Default Security Protocol**

2    7.3.1 Overview

3    The Default Security Protocol does not provide any services, except for transferring packets  
 4    between the Authentication Protocol and the MAC layer.

5    7.3.2 Basic Protocol Numbers

6    The Subtype field for this protocol is two octets set to  $N_{SPDefault}$ .

7    7.3.3 Protocol Data Unit

8    The protocol data unit for this protocol is a Security Layer packet. Each Security Layer  
 9    packet consists of an Authentication Protocol packet.

10   The protocol shall set the Security Layer packet to the Authentication Protocol packet and  
   11   shall forward it for transmission to the MAC Layer. This protocol does not define a Security  
   12   Protocol header or trailer.

13   This protocol shall set the Authentication Protocol packet to the Security Layer packet  
   14   received from the MAC Layer, and shall forward the packet to the Authentication Protocol.

15   7.3.4 Default Security Protocol Header

16   The Default Security Protocol does not add a header.

17   7.3.5 Default Security Protocol Trailer

18   The Default Security Protocol does not add a trailer.

19   7.3.6 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
$N_{SPType}$	Type field for this protocol	Table 2.3.6-1
$N_{SPDefault}$	Subtype field for this protocol	0x0000

20

21

1   **7.4 Generic Security Protocol**

2    7.4.1 Overview

3   The Generic Security protocol performs the following tasks:

- 4       • On the transmission side, this protocol provides a Time Stamp that may be used by  
5       the negotiated Authentication Protocol and Encryption Protocol.
- 6       • On the receiving side, this protocol computes the Time Stamp using the information  
7       provided in the Security Protocol header and makes the Time Stamp publicly  
8       available.

9    7.4.2 Basic Protocol Numbers

10   The Subtype field for this protocol is two octets set to  $N_{SPGeneric}$ .

11   7.4.3 Protocol Data Unit

12   The protocol data unit for this protocol is a Security Layer packet. Each Security Layer  
13   packet consists of an Authentication Protocol packet and a Security Protocol header.

14   The protocol shall construct a Security Layer packet out of the Authentication Protocol  
15   packet as follows and shall pass the packets for transmission to the MAC Layer:

- 16       • When the protocol receives an Authentication Protocol packet from the  
17       Authentication Protocol that is either authenticated or encrypted, it shall set  
18       TimeStampShort in the Security protocol header to the least significant 16 bits of the  
19       value of the TimeStampLong that is used by the Authentication Protocol or the  
20       Encryption Protocol to authenticate or encrypt this packet. The Security Protocol  
21       shall then add the Security Protocol header in front of the Authentication Protocol  
22       packet. The packet structure is shown in Figure 7.2-1.
- 23       • When the protocol receives an Authentication Protocol packet from the  
24       Authentication Protocol that is neither authenticated nor encrypted, the protocol  
25       shall not add a security protocol header to the Authentication Protocol packet.
- 26       • This protocol shall not append a Security Protocol trailer to the Authentication  
27       Protocol packet.

28   This Security Protocol shall construct the Authentication Protocol packet using the Security  
29   Layer packet (received from the MAC Layer) as follows and shall forward the packet to the  
30   Authentication Protocol:

- 31       • When the protocol receives a Security Layer packet from the MAC Layer that is either  
32       authenticated or encrypted, it shall construct the Authentication Protocol packet by  
33       removing the Security Layer header.
- 34       • When the protocol receives a Security Layer packet from the MAC Layer that is  
35       neither authenticated nor encrypted, it shall set the Authentication Protocol packet  
36       to the Security Layer packet.

1    7.4.4 Procedures

2    When the Security Layer receives a Connection Layer packet that is to be either  
 3    authenticated or encrypted, the Security Protocol shall choose a value for the  
 4    TimeStampLong based on the current 64-bit representation of the CDMA System Time in  
 5    units of 80 ms, such that TimeStampLong does not specify a time later than the time that  
 6    the security layer packet will be transmitted by the physical layer, and is not earlier than  
 7    the current CDMA System Time<sup>36</sup>. The protocol shall then set TimeStampShort in the  
 8    Security Protocol header to TimeStampLong[15:0].

9    When the Security Protocol receives a Security Layer packet from the MAC Layer that is  
 10   either authenticated or encrypted, it shall compute the 64-bit TimeStampLong using  
 11   TimeStampShort given in the Security Protocol Header as follows:

12       $\text{TimeStampLong} = (\text{SystemTime} - (\text{SystemTime}[15:0] - \text{TimeStampShort}) \bmod 2^{16})$   
 13       $\bmod 2^{64}$ ,

14      where SystemTime is the current CDMA System Time in units of 80 ms,  
 15      SystemTime[15:0] is the 16 least significant bits of the SystemTime, and  
 16      TimeStampShort is the 16-bit Security protocol header.

17    7.4.5 Generic Security Protocol Header

18      The Generic Security Protocol Header is as follows:

<b>Field</b>	<b>Length(bits)</b>
TimeStampShort	0 or 16

20      TimeStampShort      The sender shall include this field, only if the Authentication Protocol  
 21      packet is either authenticated or encrypted. The sender shall set this  
 22      field to the 16 least significant bits of the TimeStampLong.

23    7.4.6 Generic Security Protocol Trailer

24      The Generic Security Protocol does not add a trailer.

25    7.4.7 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
NsPType	Type field for this protocol	Table 2.3.6-1
NsPGeneric	Subtype field for this protocol	0x0001

---

26  
 27      <sup>36</sup> For example, the protocol may choose the current CDMA System Time as TimeStampLong.

**1    7.5 Default Key Exchange Protocol****2    7.5.1 Overview**

3    The Default Key Exchange Protocol does not provide any services and is selected when the  
4    Default Authentication Protocol and the Null encryption Protocol are selected.

**5    7.5.2 Basic Protocol Numbers**

6    The Subtype field for this protocol is two octets and is set to N<sub>KEPDefault</sub>.

**7    7.5.2.1 Initialization**

8    The protocol in the access terminal and access network shall set all of the following  
9    variables to NULL:

- 10      • SKey
- 11      • FACAAuthKey
- 12      • RACAAuthKey
- 13      • FACEncKey
- 14      • RACEncKey
- 15      • FPCAuthKey
- 16      • RPCAuthKey
- 17      • FPCEncKey
- 18      • RPCEncKey

**19    7.5.3 Protocol Data Unit**

20    This protocol does not carry payload on behalf of other layers or protocols.

**21    7.5.4 Protocol Numeric Constants**

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>KEPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>KEPDefault</sub>	Subtype field for this protocol	0x0000

23

24

**7.6 DH Key Exchange Protocol**

## 7.6.1 Overview

The DH Key Exchange Protocol provides a method for session key exchange based on Diffie-Hellman (DH).

## 7.6.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets and is set to N<sub>KEPDH</sub>.

## 7.6.3 Protocol Data Unit

The transmission unit of this protocol is a message. This is a control protocol and, therefore, it does not carry payload on behalf of other layers or protocols.

This protocol uses the Signaling Application to transmit and receive messages.

## 7.6.4 Procedures

The Key Exchange Protocol uses the KeyRequest and KeyResponse messages for exchanging public session keys, and the ANKeyComplete and ATKeyComplete messages for indicating that the secret session keys have been calculated.

The access terminal and the access network shall perform the following key exchange procedure during session configuration.

## 7.6.4.1 Initialization

The protocol in the access terminal and access network shall initialize all the following variables to NULL:

- SKey
- FACAAuthKey
- RACAAuthKey
- FACEEncKey
- RACEncKey
- FPCAuthKey
- RPCAuthKey
- FPCEncKey
- RPCEncKey

## 7.6.4.2 Access Network Requirements

The access network shall initiate the key exchange by sending a KeyRequest message. The access network shall choose a random number ANRand between KeyLength and  $2^{\text{KeyLength}} - 2$  and set the ANPubKey field of the KeyRequest message as follows:

1            $\text{ANPubKey} = g^{\text{ANRand}} \bmod p$

2       where  $g$ ,  $p$ , and  $\text{KeyLength}$  are specified during session configuration of the DH Key  
3       Exchange Protocol.

4       The random number  $\text{ANRand}$  should have the following properties:

- 5       • The number generated should have a uniform statistical distribution over its range.
- 6       • The numbers used in formulating different  $\text{KeyRequest}$  messages should be  
7       statistically uncorrelated.
- 8       • The number used in formulating each  $\text{KeyRequest}$  message should not be derivable  
9       from the previously used random numbers.
- 10      • The numbers used in formulating  $\text{KeyRequest}$  message sent by different access  
11     networks should be statistically uncorrelated.

12      If the access network does not receive a  $\text{KeyResponse}$  message with a  $\text{TransactionID}$  field  
13     that matches the  $\text{TransactionID}$  field of the associated  $\text{KeyRequest}$  message, within  
14      $T_{\text{KEPANResponse}}$ , the access network shall declare failure and stop performing the rest of the  
15     key exchange procedure.

16      After receiving a  $\text{KeyResponse}$  message with a  $\text{TransactionID}$  field that matches the  
17      $\text{TransactionID}$  field of the associated  $\text{KeyRequest}$  message, the access network shall  
18     perform the following:

- 19       • The access network shall set  $T_{\text{KEPKeyCompAT}}$  to the duration of time specified by  
20       Timeout, reported by the access terminal in the  $\text{KeyResponse}$  message. The access  
21       network shall then start the AT Key Computation Timer with a time-out value of  
22        $T_{\text{KEPKeyCompAT}}$ .
- 23       • The access network shall compute  $S\text{Key}$ , the session key as follows:

24            $S\text{Key} = \text{ATPubKey}^{\text{ANRand}} \bmod p$

- 25       • The access network shall construct the *message bits*, as shown in Table 7.6.4.2-1,  
26       using the computed  $S\text{Key}$ ,  $\text{TimeStampLong}$ , the  $\text{TransactionID}$ , and a 16-bit pseudo-  
27       random value,  $\text{Nonce}$ .  $\text{TimeStampLong}$  is a 64-bit value that is set, based on the  
28       current 64-bit representation of the CDMA System Time in units of 80 ms, such that  
29        $\text{TimeStampLong}$  does not specify a time later than the time that the message will be  
30       transmitted by physical layer and is not earlier than the current CDMA System  
31       Time<sup>37</sup>.

---

<sup>37</sup> For example, the protocol may choose the current CDMA System Time as  $\text{TimeStampLong}$ .

**Table 7.6.4.2-1. Message Bits**

<b>Field</b>	<b>Length(bits)</b>
SKey	KeyLength
TransactionID	8
Nonce	16
TimeStampLong	64

- The access network shall pad the *message bits* constructed in the previous step, as specified in [6], and compute the 160-bit *message digest* as specified in [6].
- The access network shall send an ANKeyComplete message with the KeySignature field of the message set to the *message digest* computed in the previous step and the TimeStampShort field of the message set to the 16 least significant bits of the CDMA System Time used in the previous step. The access network shall then start the AT Signature Computation Timer with a time-out value of T<sub>KEPSigCompAN</sub>.

The access network shall disable both the AT Key Computation Timer and the AT Key Signature Computation Timer when it receives an ATKeyComplete message with a TransactionID that matches the TransactionID field of the associated KeyRequest and KeyResponse messages.

The access network shall declare failure and stop performing the rest of the key exchange procedure if any of the following events occur:

- Both AT Key Computation and the AT Key Signature Computation Timers are expired, or
- Access network receives an ATKeyComplete message with Result field set to '0'.

#### 7.6.4.3 Access Terminal Requirements

Upon receiving the KeyRequest message, the access terminal shall perform the following:

- The access terminal shall choose a random number ATRand between KeyLength and  $2^{\text{KeyLength}} - 2$  and set the ATPubKey field of the KeyResponse message as follows:

$$\text{ATPubKey} = g^{\text{ATRand}} \bmod p$$

where  $g$  and  $p$  are KeyLength dependent protocol constants for the DH Key Exchange protocol, and KeyLength is specified during session configuration of the DH Key Exchange Protocol.

- The access terminal shall send a KeyResponse message with the ATPubKey field set to the value computed in the previous step, within T<sub>KEPATResponse</sub> second of receiving a KeyRequest message.
- The access terminal shall compute SKey, the session key as follows:

$$\text{SKey} = \text{ANPubKey}^{\text{ATRand}} \bmod p.$$

The random number ATRand should have the following properties:

- Number generated should have a uniform statistical distribution over its range,
  - Numbers used in formulating different KeyResponse messages should be statistically uncorrelated,
  - Number used in formulating each KeyResponse message should not be derivable from the previously used random numbers,
  - Numbers used in formulating KeyResponse message sent by different access terminals should be statistically uncorrelated.

After the access terminal sends a KeyResponse message, it shall set  $T_{KEPKeyCompAN}$  to the duration of time specified by Timeout, reported by the access network in the KeyRequest message. The access terminal shall then start the AN Key Computation Timer with a timeout value of  $T_{KEPKeyCompAN}$ . The access terminal shall disable the AN Key Computation Timer when it receives the ANKeyComplete message with a TransactionID that matches the TransactionID field of the associated KeyRequest and KeyResponse messages.

When the AN Key Computation Timer expires, the access terminal shall declare failure.

After receiving an ANKeyComplete message with a TransactionID field that matches the TransactionID field of the associated KeyRequest message, the access terminal shall perform the following:

- Access terminal shall compute the 64-bit variable TimeStampLong as follows:  

$$\text{TimeStampLong} = (\text{SystemTime} - (\text{SystemTime}[15:0] - \text{TimeStampShort}) \bmod 2^{16}) \bmod 2^{64},$$

where SystemTime is the current CDMA System Time in units of 80 ms, SystemTime[15:0] is the 16 least significant bits of the SystemTime, and TimeStampShort is the 16-bit field received in the ANKeyComplete message.
  - Access terminal shall construct the *message bits* as shown in Table 7.6.4.3-1 using the computed SKey, computed TimeStampLong, and TransactionID, and Nonce fields of the ANKeyComplete message.

**Table 7.6.4.3-1. Message Bits**

<b>Field</b>	<b>Length(bits)</b>
Skey	KeyLength
TransactionID	8
Nonce	16
TimeStampLong	64

- Access terminal shall pad the *message bits* constructed in the previous step, as specified in [6], and compute the 160-bit *message digest* as specified in [6].

- If the *message digest* computed in the previous step matches the KeySignature field of ANKeyComplete message, the access terminal shall send an ATKeyComplete message with the Result field set to ‘1’ within  $T_{KEPSigCompAT}$  seconds of the latter of the following two events:
  - Reception of the ANKeyComplete message.
  - Finishing computing the SKey.
- Otherwise, the access terminal shall declare failure and send an ATKeyComplete message with the Result field set to ‘0’.

#### 7.6.4.4 Authentication Key and Encryption Key Generation

The keys used for authentication and encryption are generated from the session key, SKey, using the procedures specified in this section.

Table 7.6.4.4-1 defines eight sub-fields within the SKey. These sub-fields are of equal length.

**Table 7.6.4.4-1. Subfields of SKey**

<b>Sub-Field</b>	<b>Length (bits)</b>
K0	KeyLength / 8
K1	KeyLength / 8
K2	KeyLength / 8
K3	KeyLength / 8
K4	KeyLength / 8
K5	KeyLength / 8
K6	KeyLength / 8
K7	KeyLength / 8

The access network and access terminal shall construct the *message bits* as shown in Figure 7.6.4.4-1. In this figure, TimeStampLong and Nonce are the same as the one used for generation of KeySignature (see 7.6.4.2, and 7.6.4.3).

	MSB		LSB
<b>Message bits for generation of FACAAuthKey</b>	K0 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of RACAuthKey</b>	K1 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of FACEEncKey</b>	K2 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of RACEncKey</b>	K3 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of FPCAuthKey</b>	K4 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of RPCAuthKey</b>	K5 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of FPCEncKey</b>	K6 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)
<b>Message bits for generation of RPCEncKey</b>	K7 (KeyLength / 8)	Nonce (16 bits)	TimeStampLong (64 bits)

**Figure 7.6.4.4-1. Message Bits for Generation of Authentication and Encryption Keys**

The access terminal and access network shall then pad the *message bits* constructed in the previous step, as specified in [6], and compute the 160-bit *message digests* (for each of the eight keys) as specified in [6]. The access network and access terminal shall set the FACAAuthKey, RACAuthKey, FACEEncKey, RACEncKey, FPCAuthKey, RPCAuthKey, FPCEncKey, and RPCEncKey to the *message digests* for the corresponding key as shown in Figure 7.6.4.4-1.

## 7.6.5 Message Formats

### 7.6.5.1 KeyRequest

The access network sends the KeyRequest message to initiate the session key exchange.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
TransactionID	8
Timeout	8
ANPubKey	KeyLength (as negotiated)

- 1    MessageID                 The access network shall set this field to 0x00.
- 2    TransactionID            The access network shall increment this value for each new  
3                              KeyRequest message sent.
- 4    Timeout                  Shared secret calculation timeout. The access network shall set this  
5                              field to the maximum time in the number of seconds that the access  
6                              network requires for calculation of the session key (SKey).
- 7    ANPubKey                Access network's ephemeral public Diffie-Hellman key. The access  
8                              network shall set this field to the ephemeral public Diffie-Hellman key  
9                              of the access network as specified in 7.6.4.2.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

- 11    7.6.5.2 KeyResponse
- 12    The access terminal sends the KeyResponse message in response to the KeyRequest  
13                              message.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
TransactionID	8
Timeout	8
ATPubKey	KeyLength (as negotiated)

- 15    MessageID                The access terminal shall set this field to 0x01.
- 16    TransactionID           The access terminal shall set this field to the value of the  
17                              TransactionID field of the KeyRequest message to which the access  
18                              terminal is responding.

1      Timeout                         Shared secret calculation timeout. The access terminal shall set this  
 2                                        field to the maximum time in seconds that the access terminal  
 3                                        requires for calculation of the session key (SKey).

4      ATPubKey                       Access terminal's ephemeral public Diffie-Hellman key. The access  
 5                                        terminal shall set this field to the ephemeral public Diffie-Hellman  
 6                                        key of the access terminal as specified in 7.6.4.3.

<b>Channels</b>	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

8      7.6.5.3 ANKeyComplete

9      The access network sends the ANKeyComplete message in response to the KeyResponse  
 10                                        message.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
TransactionID	8
Nonce	16
TimeStampShort	16
KeySignature	160

12     MessageID                       The access network shall set this field to 0x02.

13     TransactionID                  The access network shall set this field to the value of the  
 14                                        TransactionID field of the corresponding KeyRequest message.

15     Nonce                           The access network shall set this field to an arbitrarily chosen 16-bit  
 16                                        value Nonce that is used to compute the KeySignature.

17     TimeStampShort                The access network shall set this field to the 16 least significant bits  
 18                                        of the SystemTimeLong used in computing the KeySignature as  
 19                                        specified in 7.6.4.2.

20     KeySignature                  The access network shall set this field to the 20-octet signature of the  
 21                                        session key (SKey) as specified in 7.6.4.2.  
 22

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

## 1    7.6.5.4 ATKeyComplete

2    The access terminal sends the ATKeyComplete message in response to the ANKeyComplete  
3    message.

4

Field	Length (bits)
MessageID	8
TransactionID	8
Result	1
Reserved	7

5    MessageID         The access terminal shall set this field to 0x03.

6    TransactionID     The access terminal shall set this field to the value of the  
7                      TransactionID field of the corresponding KeyRequest message.8    Result             The access terminal shall set this field to ‘1’ if the KeySignature field  
9                      of ANKeyComplete message matches the *message digest* computed for  
10                     the KeySignature as specified in 7.6.4.3; otherwise the access  
11                     terminal shall set this field to ‘0’.12   Reserved          The access terminal shall set this field to zero. The access network  
13                     shall ignore this field.  
14

<b>Channels</b>		RTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

## 15   7.6.5.5 Configuration Messages

16   The DH Key Exchange Protocol uses the Generic Configuration Protocol for configuration.  
17   All configuration messages sent by this protocol shall have their Type field set to  $N_{KEPType}$ .

18   Unless stated otherwise, all attributes are simple attributes.

19   The configurable attributes for this protocol are listed in Table 7.6.5.5-1.

20   The access terminal shall use as defaults the values Table 7.6.5.5-1 typed in ***bold italics***.

**Table 7.6.5.5-1. Configurable Values**

<b>Attribute ID</b>	<b>Attribute</b>	<b>Values</b>	<b>Meaning</b>
0x00	Session Key Length (KeyLength)	<b>0x00</b>	Default is 96-octet (768-bit) Diffie-Hellman key. KeyLength = 768
		0x01	128-octet (1024-bit) Diffie-Hellman key. KeyLength = 1024
		0x02-0xff	Reserved

## 2    7.6.5.5.1 ConfigurationRequest

3    The sender sends the ConfigurationRequest message to request the configuration of one or  
 4    more parameters for the Key Exchange Protocol. The ConfigurationRequest message format  
 5    is given as part of the Generic Configuration Protocol (see 10.7).

6    The sender shall set the MessageID field of this message to 0x50.

<b>Channels</b>	FTC      RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

## 8    7.6.5.5.2 ConfigurationResponse

9    The sender sends the ConfigurationResponse message to select one of the parameter  
 10   settings offered in an associated ConfigurationRequest message. The  
      ConfigurationResponse message format is given as part of the Generic Configuration  
 12   Protocol (see 10.7).

13   The sender shall set the MessageID field of this message to 0x51.

<b>Channels</b>	FTC      RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

1    7.6.6 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>KEPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>KEPDH</sub>	Subtype field for this protocol	0x0001
T <sub>KEPSigCompAN</sub>	Time to receive ATKeyComplete after sending ANKeyComplete	3.5 seconds
T <sub>KEPSigCompAT</sub>	Time to send ATKeyComplete after receiving ANKeyComplete	3 seconds
T <sub>KEPANResponse</sub>	Time to receive KeyResponse after sending KeyRequest	3.5 seconds
T <sub>KEPATResponse</sub>	Time to send KeyResponse after receiving KeyRequest	3 second

2

1      **Table 7.6.5.5-1. Common Primitive Base and Common Prime Modulus for KeyLength**  
 2      **equal to 768<sup>38</sup>**

Constant	Meaning	Value				
g	Common primitive base	0x02				
p	Common prime modulus (MSB first)	0xFFFFFFFF	0xFFFFFFFF	0xC90FDAA2	0x2168C234	0xC4C6628B
		0x29024E08	0x8A67CC74	0x80DC1CD1	0x3B139B22	0x514A0879
		0xEF9519B3	0xCD3A431B	0x020BBEA6	0xF25F1437	0x4FE1356D
		0xE485B576	0x625E7EC6	0x302B0A6D	0xA63A3620	0xF44C42E9
		0xFFFFFFFF	0xFFFFFFFF	0x6D51C245		0xFFFFFFFF

3

4      **Table 7.6.5.5-2. Common Primitive Base and Common Prime Modulus for KeyLength**  
 5      **equal to 1024**

Constant	Meaning	Value				
g	Common primitive base	0x02				
p	Common prime modulus (MSB first)	0xFFFFFFFF	0xFFFFFFFF	0xC90FDAA2	0x2168C234	0xC4C6628B
		0x29024E08	0x8A67CC74	0x80DC1CD1	0x3B139B22	0x514A0879
		0xEF9519B3	0xCD3A431B	0x020BBEA6	0xF25F1437	0x4FE1356D
		0xE485B576	0x625E7EC6	0x302B0A6D	0xA637ED6B	0x0BFF5CB6
		0xEE386BFB	0x5A899FA5	0xF406B7ED	0x7C4B1FE6	0x49286651
		0xFFFFFFFF	0xFFFFFFFF	0xAE9F2411		0xECE65381

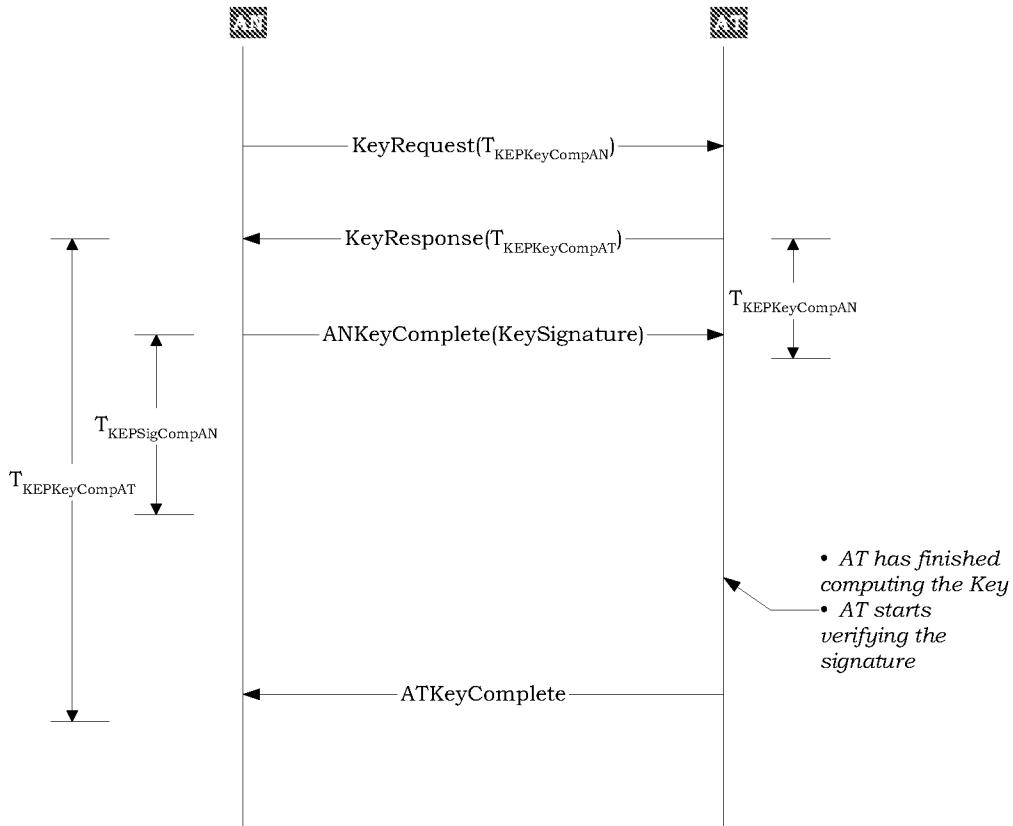
6

### 7.6.7 Message Flows

7      Figure 7.6.7-1 shows an example flow diagram in which the access network quickly  
 8      computes the Key and the signature and sends it to the access terminal. The access  
 9      terminal still needs time to finish the Key calculation. In this case the *AT Signature*  
 10     *Computation Timer* expires, but the *AT Key Computation Timer* does not expire.

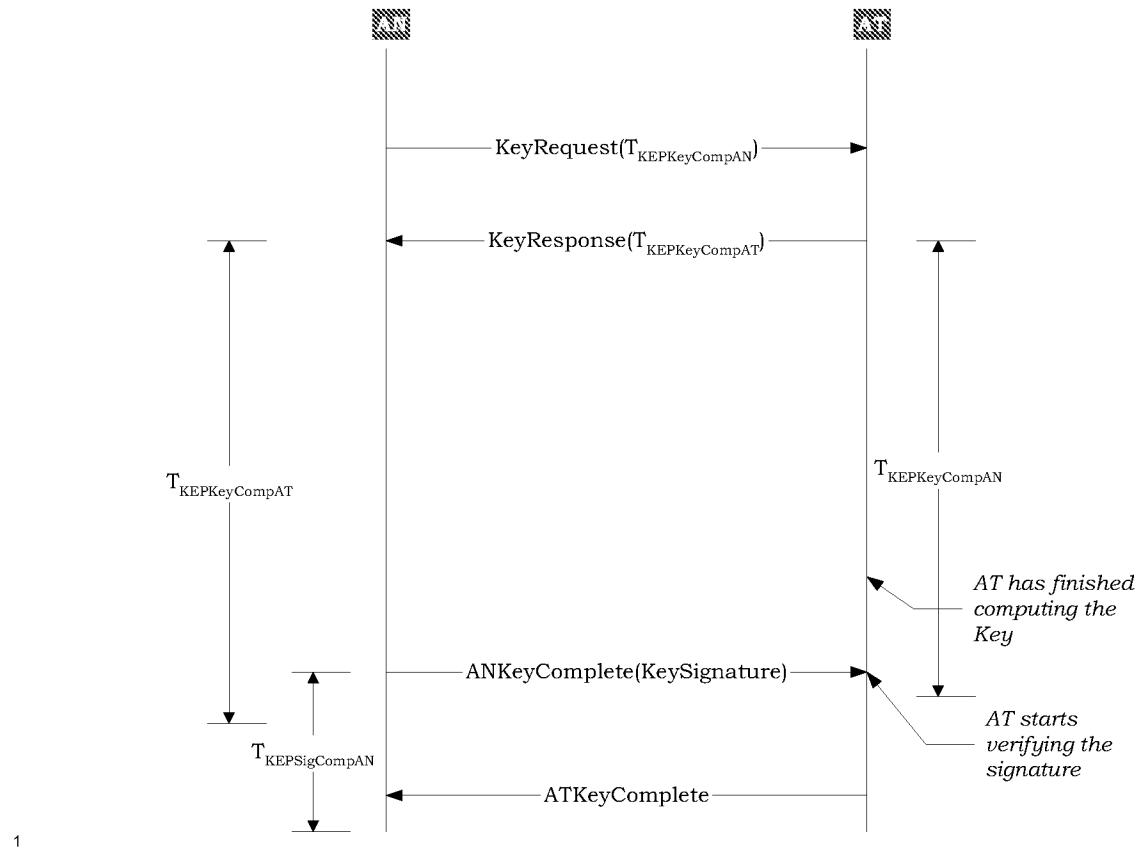
---

38 The values for p and g are taken from [7].



**Figure 7.6.7-1. Example Call Flow: Timer  $T_{KEPSigCompAN}$  Expires But  $T_{KEPKeyCompAT}$  Does Not Expire**

Figure 7.6.7-2 shows an example flow diagram in which the access network requires a longer period of time to compute the Key. In this case the *AT Key Computation Timer* expires, but the *AT Signature Computation Timer* does not expire.



**Figure 7.6.7-2. Example Call Flow: Timer  $T_{KEPSigCompAN}$  Does Not Expire But  $T_{KEPKeyCompAT}$  Expires**

1   **7.7 Default Authentication Protocol**

2    7.7.1 Overview

3    The Default Authentication Protocol does not provide any services except for transferring  
4    packets between the Encryption Protocol and the Security Protocol.

5    7.7.2 Basic Protocol Numbers

6    The Subtype field for this protocol is two octets set to  $N_{APDefault}$ .

7    7.7.3 Protocol Data Unit

8    The protocol data unit for this protocol is an Authentication Protocol packet.

9    When this protocol receives Encryption Protocol packets, it shall forward them to the  
10   Security Protocol.

11   When the protocol receives a Security Protocol packet from the Security Protocol, it shall set  
12   the Encryption Protocol packet to the Authentication Protocol packet and shall forward the  
13   Encryption Protocol packet to the Encryption Protocol.

14   7.7.4 Default Authentication Protocol Header

15   The Default Authentication Protocol does not add a header.

16   7.7.5 Default Authentication Protocol Trailer

17   The Default Authentication Protocol does not add a trailer.

18   7.7.6 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
$N_{APType}$	Type field for this protocol	Table 2.3.6-1
$N_{APDefault}$	Subtype field for this protocol	0x0000

20

21

**7.8 SHA-1 Authentication Protocol**

## 7.8.1 Overview

The SHA-1 Authentication Protocol provides a method for authentication of the Access Channel MAC Layer packets by applying the SHA-1 hash function to *message bits* that are composed of the ACAuthKey, security layer payload, CDMA System Time, and the sector ID.

## 7.8.2 Basic Protocol Numbers

The Subtype field for this protocol is two octets set to N<sub>APSHA1</sub>.

## 7.8.3 Protocol Data Unit

The protocol data unit for this protocol is an Authentication Protocol packet. This protocol receives Encryption Protocol Packets and adds the authentication layer header defined in 7.8.5 in front of each Access Channel Encryption Protocol Packet to make an Access Channel Authentication Protocol Packet and forwards it to the Security protocol.

When the protocol receives Access Channel Security protocol packets from the Security protocol, it constructs the Encryption Protocol Packet by removing the Authentication Protocol Header, and forwards the Encryption Protocol Packet to the Encryption Protocol.

## 7.8.4 Procedures

The procedures in 7.8.4.1 and 7.8.4.2 shall apply to packets carried by the Access Channel. For all other packets, the Default Authentication Protocol defined in 7.7 shall apply.

## 7.8.4.1 Access Network Requirements

Upon reception of an Authentication Protocol packet from the Access Channel, the access network shall compute and verify the Access Channel MAC Layer packet authentication code (ACPAC) given in the authentication protocol header as follows:

- The access network shall construct the ACAuthKey from the RPCAuthKey public data of the Key Exchange Protocol as follows:
  - If the length of RPCAuthKey is equal to the length of ACAuthKey, then ACAuthKey shall be RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is greater than the length of ACAuthKey, then ACAuthKey shall be the ACAuthKeyLength least significant bits of RPCAuthKey.
  - Otherwise, if the length of RPCAuthKey is less than the length of ACAuthKey, then ACAuthKey shall be set to RPCAuthKey with zeros concatenated to the end (LSB) of it, such that the length of the result is ACAuthKeyLength.
- The access network shall construct the *message bits* for computing ACPAC as shown in Table 7.8.4.1-1:

1  
**Table 7.8.4.1-1. Message Bits for ACPAC Computation**

<b>Field</b>	<b>Length(bits)</b>
ACAuthKey	ACAuthKeyLength
Authentication Protocol Payload	variable
SectorID	128
TimeStampLong	64

2 where SectorID is provided as public data by the Overhead Messages protocol and  
 3 TimeStampLong is the 64-bit public value provided by the Security layer protocol.

- 4
- 5 The access network shall pad the *message bits* constructed in the previous step, as  
 6 specified in [6], and compute the 160-bit *message digest* as specified in [6] and set  
 ACPAC to the 64 least significant bits of the *message digest*.

7 If the ACPAC computed in the previous step matches the ACPAC field in the Protocol  
 8 Header, then the Protocol shall deliver the Authentication Layer Payload to the Encryption  
 9 Protocol. Otherwise, the Protocol shall issue a *Failed* indication and shall discard the  
 10 security layer packet.

11 7.8.4.2 Access Terminal Requirements

12 Upon reception of an Encryption Protocol packet destined for the Access Channel, the  
 13 access terminal shall compute ACPAC as follows:

- 14
- 15 The access terminal shall construct the ACAuthKey from the RPCAuthKey public  
 data of the Key Exchange Protocol as follows:
    - 16 – If the length of RPCAuthKey is equal to the length of ACAuthKey, then ACAuthKey  
 shall be RPCAuthKey.
    - 17 – Otherwise, if the length of RPCAuthKey is greater than the length of ACAuthKey,  
 then ACAuthKey shall be the ACAuthKeyLength least significant bits of  
 RPCAuthKey.
    - 18 – Otherwise, if the length of RPCAuthKey is less than the length of ACAuthKey, then  
 ACAuthKey shall be the concatenation of zeros at the end (LSB) of RPCAuthKey,  
 such that the length of the result is ACAuthKeyLength.
  - 21 The access terminal shall construct the *message bits* for computing ACPAC as shown  
 22 in Table 7.8.4.2-1:  
 23

1                   **Table 7.8.4.2-1. Message Bits for ACPAC Computation**

<b>Field</b>	<b>Length(bits)</b>
ACAuthKey	ACAuthKeyLength
Authentication Protocol Payload	variable
SectorID	128
TimeStampLong	64

2                   where SectorID is provided as public data by the Overhead Messages Protocol and  
 3                   TimeStampLong is the 64-bit public value provided by the Security Protocol.

- 4                   • The access terminal shall pad the *message bits* constructed in the previous step, as  
 5                   specified in [6], and compute the 160-bit *message digest* as specified in [6] and set  
 6                   the ACPAC field to the 64 least significant bits of the *message digest*.

7                   7.8.5 SHA-1 Authentication Protocol Header Format

8                   The SHA-1 Authentication Protocol is as follows:

<b>Field</b>	<b>Length(bits)</b>
ACPAC	64

10          ACPAC                   Access Channel Packet Authentication Code. The access terminal  
 11                                shall compute this field as specified in 7.8.4.2.

12                   7.8.6 SHA-1 Authentication Protocol Trailer

13                   The SHA-1 Authentication Protocol does not add a trailer.

14                   7.8.6.1 Configuration Messages

15          The SHA-1 Authentication Protocol uses the Generic Configuration Protocol for  
 16                                configuration. All configuration messages sent by this protocol shall have their Type field  
 17                                set to NAPType.

18                   Unless stated otherwise, all attributes are simple attributes.

19                   The configurable attributes for this protocol are listed in Table 7.8.6.1-1.

20                   The access terminal shall use as defaults the values Table 7.8.6.1-1 typed in ***bold italics***.

1  
**Table 7.8.6.1-1. Configurable Values**

<b>Attribute ID</b>	<b>Attribute</b>	<b>Values</b>	<b>Meaning</b>
0x00	ACAuthKeyLength	<b>0x00A0</b>	Default value for the authentication key length in bits.
		0x0000 – 0xFFFF	Access Channel authentication key length in bits.

2  
**7.8.6.1.1 ConfigurationRequest**

3 The sender sends the ConfigurationRequest message to request the configuration of one or  
4 more parameters for the Authentication Protocol. The ConfigurationRequest message format  
5 is given as part of the Generic Configuration Protocol (see 10.7).

6 The sender shall set the MessageID field of this message to 0x50.

<b>Channels</b>	FTC      RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

8  
**7.8.6.1.2 ConfigurationResponse**

9 The sender sends the ConfigurationResponse message to select one of the parameter  
10 settings offered in an associated ConfigurationRequest message. The  
11 ConfigurationResponse message format is given as part of the Generic Configuration  
12 Protocol (see 10.7).

13 The sender shall set the MessageID field of this message to 0x51.

<b>Channels</b>	FTC      RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

15  
**7.8.7 Protocol Numeric Constants**

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>APType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>APSHA1</sub>	Subtype field for this protocol	0x0001

**7.9 Default Encryption Protocol**

The Default Encryption Protocol does not alter the Security Layer packet payload (i.e., no encryption/decryption) and does not add an Encryption Protocol Header or Trailer; therefore, the Cipher-text for this protocol is equal to the Connection Layer packet. If needed, end-to-end encryption can be provided at the application layer (which is outside the scope of this specification).

**7.9.1 Basic Protocol Numbers**

The Subtype field for this protocol is two octets set to  $N_{EPDefault}$ .

**7.9.2 Protocol Data Unit**

The protocol data unit for this protocol is an Encryption Protocol Packet. The Encryption Protocol Packet for this protocol is the same as the Connection Layer packet.

**7.9.3 Default Encryption Protocol Header**

The Default Encryption Protocol does not add a header.

**7.9.4 Default Encryption Protocol Trailer**

The Default Encryption Protocol does not add a trailer.

**7.9.5 Protocol Numeric Constants**

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
$N_{EPType}$	Type field for this protocol	Table 2.3.6-1
$N_{EPDefault}$	Subtype field for this protocol	0x0000

- 1 No text.

## 8 MAC LAYER

### 8.1 Introduction

#### 8.1.1 General Overview

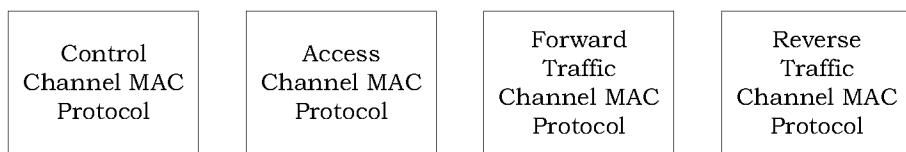
The MAC Layer contains the rules governing operation of the Control Channel, Access Channel, Forward Traffic Channel, and Reverse Traffic Channel.

This section presents the default protocols for the MAC Layer. Each of these protocols can be independently negotiated at the beginning of the session.

The MAC Layer contains the following protocols:

- Control Channel MAC Protocol: This protocol builds Control Channel MAC Layer packets out of one or more Security Layer packets, contains the rules concerning access network transmission and packet scheduling on the Control Channel, access terminal acquisition of the Control Channel, and access terminal Control Channel MAC Layer packet reception. This protocol also adds the access terminal address to transmitted packets.
- Access Channel MAC Protocol: This protocol contains the rules governing access terminal transmission timing and power characteristics for the Access Channel.
- Forward Traffic Channel MAC Protocol: This protocol contains the rules governing operation of the Forward Traffic Channel. It dictates the rules the access terminal follows when transmitting the Data Rate Control Channel, along with the rules the access network uses to interpret this channel. The protocol supports both variable rate and fixed rate operation of the Forward Traffic Channel.
- Reverse Traffic Channel MAC Protocol: This protocol contains the rules governing operation of the Reverse Traffic Channel. It dictates the rules the access terminal follows to assist the access network in acquiring the Reverse Traffic Channel. It also dictates the rules the access terminal and the access network use to select the transmission rate used over the Reverse Traffic Channel.

The relationship between the MAC layer protocols is shown in Figure 8.1.1-1.



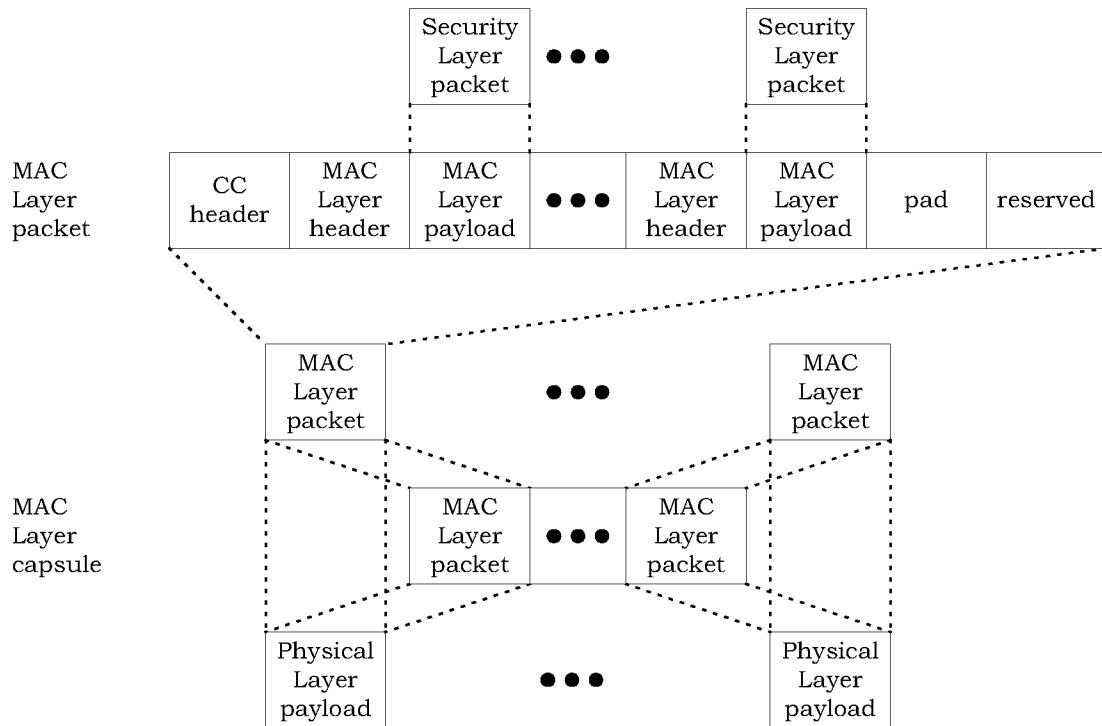
**Figure 8.1.1-1. MAC Layer Protocols**

1    8.1.2 Data Encapsulation

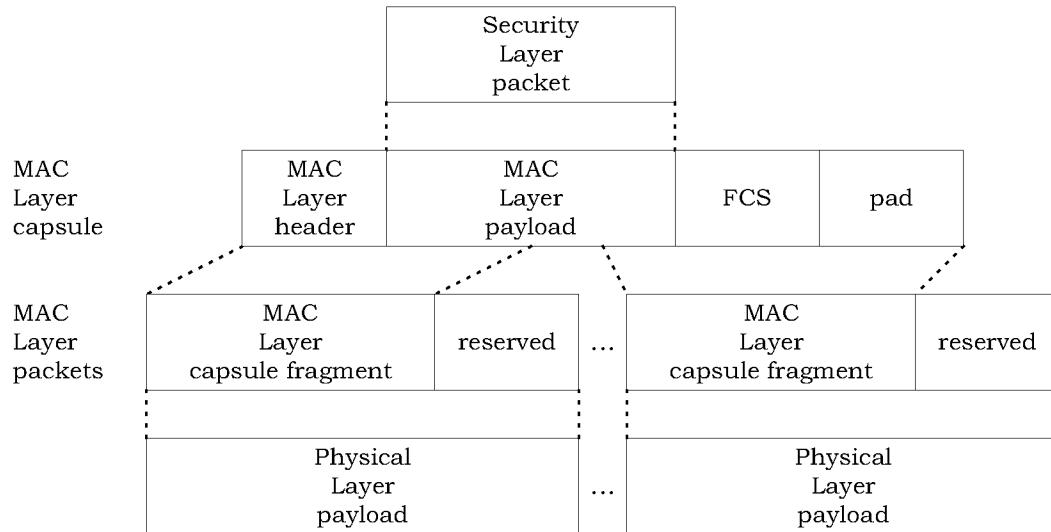
2    In the transmit direction, the MAC Layer receives Security Layer packets, adds layer-related  
3    headers, trailers and padding, and forwards the resulting packet for transmission to the  
4    Physical Layer.

5    In the receive direction, the MAC Layer receives MAC packets from the Physical Layer and  
6    forwards them to the Security Layer after removing the layer-related headers, trailers and  
7    padding.

8    Figure 8.1.2-1, Figure 8.1.2-2, Figure 8.1.2-3, and Figure 8.1.2-4 illustrate the relationship  
9    between Security Layer packets, MAC packets and Physical Layer packets for the Control  
10   Channel, Access Channel, and the Forward and Reverse Traffic Channels.

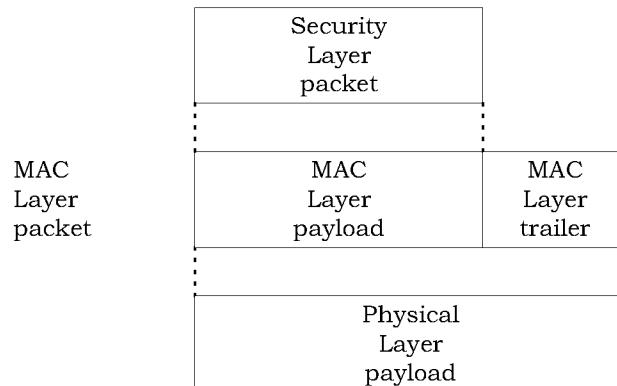


11  
12    **Figure 8.1.2-1. Control Channel MAC Layer Packet Encapsulation**



1

2

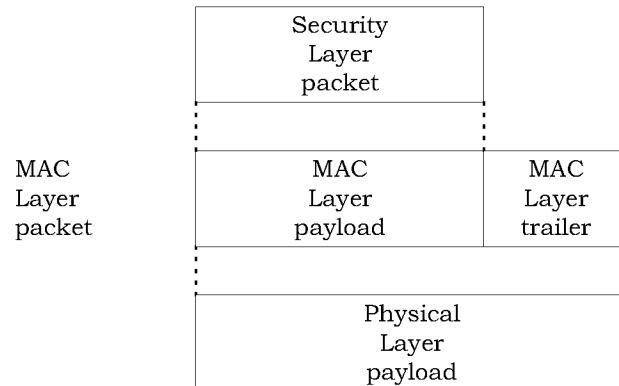
**Figure 8.1.2-2. Access Channel MAC Layer Packet Encapsulation**

3

4

**Figure 8.1.2-3. Forward Traffic Channel MAC Layer Packet Encapsulation**

5



**Figure 8.1.2-4. Reverse Traffic Channel MAC Layer Packet Encapsulation**

1  
2  
3

## 8.2 Default Control Channel MAC Protocol

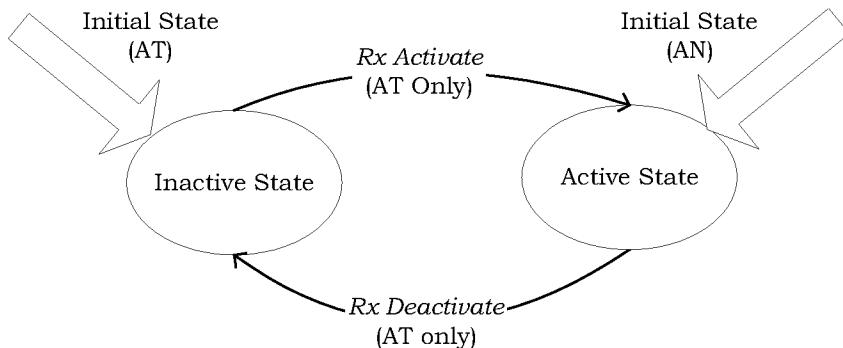
### 8.2.1 Overview

The Default Control Channel MAC Protocol provides the procedures and messages required for an access network to transmit and for an access terminal to receive the Control Channel.

This specification assumes that the access network has one instance of this protocol for all access terminals.

This protocol can be in one of two states:

- Inactive State: in this state the protocol waits for an *Activate* command. This state corresponds only to the access terminal and occurs when the access terminal has not acquired an access network or is not monitoring the Control Channel.
- Active State: in this state the access network transmits and the access terminal receives the Control Channel.



**Figure 8.2.1-1. Default Control Channel MAC Protocol State Diagram**

### 8.2.2 Primitives and Public Data

#### 8.2.2.1 Commands

This protocol defines the following commands:

- *Activate*.
- *Deactivate*.

#### 8.2.2.2 Return Indications

This protocol returns the following indications:

- *SupervisionFailed*

#### 8.2.2.3 Public Data

- None.

### 8.2.3 Basic Protocol Numbers

The Type field for this protocol is one octet, set to N<sub>CCMPType</sub>.

The Subtype field for this protocol is two octets, set to N<sub>CCMPDefault</sub>.

#### 8.2.4 Protocol Data Unit

The transmission unit of this protocol is the Control Channel MAC Layer packet. Each Control Channel MAC Layer packet consists of zero or more Security Layer packets for zero or more access terminals.

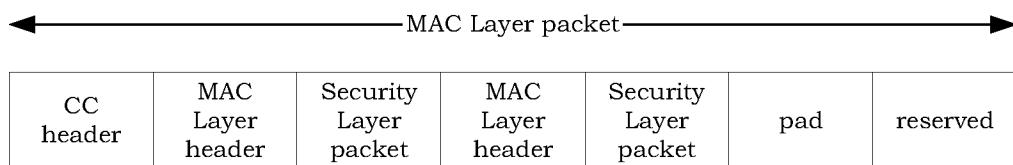
The protocol constructs a packet out of the Security Layer packets, as follows:

- It adds the MAC Layer header specified in 8.2.6.1 in front of every Security Layer packet.
  - Concatenates the Control Channel Header specified in 8.2.6.2 followed by the above formed packets.
  - Pads the resulting packet as defined in 8.2.6.3.
  - Adds the reserved bits as defined in 8.2.6.4.

The protocol then sends the packet for transmission to the Physical Layer. The packet structure is shown in Figure 8.2.4-1.

Control Channel MAC Layer packets can be transmitted, either in a synchronous capsule, which is transmitted at a particular time, or in an asynchronous capsule which can be transmitted at any time, except when a synchronous capsule is transmitted. A synchronous capsule consists of one or more Control Channel MAC Layer packets. An asynchronous capsule consists of one Control Channel MAC Layer packet.

This protocol expects an address and a parameter indicating transmission in a synchronous or an asynchronous capsule with each transmitted Security Layer packet. For Security Layer packets that are carried by an asynchronous capsule, this protocol can also receive an optional parameter indicating a transmission deadline.



**Figure 8.2.4-1. Control Channel MAC Packet Structure**

Received packets are parsed into their constituent Security Layer packets. The packets that are addressed to the access terminal (see 8.2.5.5.2.4) are then forwarded for further processing to the Security Layer.

1    8.2.5 Procedures

2    8.2.5.1 Protocol Initialization and Configuration

3    The access terminal shall start this protocol in the Inactive State.

4    The access network shall start this protocol in the Active State.

5    This protocol does not have any initial configuration requirements.

6    8.2.5.2 Command Processing

7    The access network shall ignore all commands.

8    8.2.5.2.1 Activate

9    If this protocol receives an *Activate* command in the Inactive State,

- 10    • The access terminal shall transition to the Active State
- 11    • The access network shall ignore it

12    If this protocol receives this command in the Active State it shall be ignored.

13    8.2.5.2.2 Deactivate

14    If this protocol receives a *Deactivate* command in the Inactive State, it shall be ignored.

15    If this protocol receives this command in the Active State,

- 16    • The access terminal shall transition to the Inactive State
- 17    • The access network shall ignore it

18    8.2.5.3 Control Channel Cycle

19    The Control Channel cycle is defined as a 256 slot period, synchronous with CDMA system  
20    time; i.e., there is an integer multiple of 256 slots between the beginning of a cycle and the  
21    beginning of CDMA system time.

22    8.2.5.4 Inactive State

23    This state applies only to the access terminal.

24    When the protocol is in the Inactive State, the access terminal waits for an *Activate*  
25    command.

26    8.2.5.5 Active State

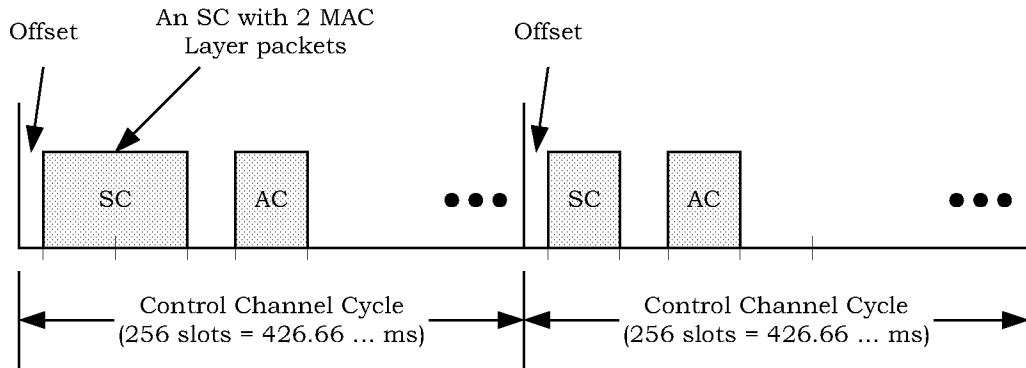
27    In this state, the access network transmits, and the access terminal monitors the Control  
28    Channel.

29    8.2.5.5.1 Access Network Requirements

30    8.2.5.5.1.1 General Requirements

31    The access network shall always have one instance of this protocol operating per sector.

- 1 When the access network transmits the Control Channel, it shall do so using a rate of 38.4  
 2 kbps or 76.8 kbps.
- 3 The access network shall transmit synchronous capsules and it may transmit  
 4 asynchronous capsules. When the access network transmits synchronous capsules, it shall  
 5 comply with 8.2.5.5.1.2. When the access network transmits asynchronous capsules, it  
 6 shall comply with 8.2.5.5.1.3.
- 7 The timing of synchronous and asynchronous capsules is shown in Figure 8.2.5.5.1.1-1.



SC: Synchronous Control Channel capsule.

AC: Asynchronous Control Channel capsule.

**Figure 8.2.5.5.1.1-1. Location of Control Channel Capsules**

#### 8.2.5.5.1.2 Transmission of Synchronous Capsules

The access network shall construct a synchronous capsule out of all the pending Security Layer packets that are destined for transmission in a synchronous capsule. The synchronous capsule may contain more than one Control Channel MAC Layer packet.

The access network shall set the SynchronousCapsule bit of the Control Channel Header to '1' only for the first Control Channel MAC Layer packet of a synchronous capsule.

The access network shall set the LastPacket bit of the Control Channel Header to '1' only for the last Control Channel MAC Layer packet of a synchronous capsule.

The access network shall set the Offset field of the Control Channel Header to the same value for all the Control Channel MAC Layer packets of a synchronous capsule.

If the access network has no pending Security Layer packets, it shall transmit a synchronous capsule with one Control Channel MAC Layer packet containing only the Control Channel header. The access network shall transmit the Control Channel MAC Layer packets of a synchronous capsule as follows:

- 1     • The first MAC Layer packet shall start transmission at times T where T satisfies the  
2       following equation:

3            $T \bmod 256 = \text{Offset}$ .

- 4     • All other MAC Layer packets of the capsule shall start transmission at the earliest  
5       time T following the end of transmission of the previous packet of the capsule that  
6       satisfies the following equation:

7            $T \bmod 4 = \text{Offset}$ ,

8       where T is CDMA System Time in slots and Offset is as specified in the Control Channel  
9       header of the packets.

10      8.2.5.5.1.3 Transmission of Asynchronous Capsules

11     The access network may transmit asynchronous capsules at any time during the Control  
12       Channel cycle in which it does not transmit a synchronous capsule. If the access network  
13       has queued Security Layer packets that are marked for transmission in an asynchronous  
14       capsule, it should transmit the packets no later than their associated transmission  
15       deadline, if one was provided. The access network may:

- 16       • Transmit these packets in a synchronous capsule.
- 17       • Transmit these packets in an asynchronous capsule.

18     The access network shall set the SynchronousCapsule bit of the Control Channel Header to  
19       ‘0’ for the Control Channel MAC Layer packet of an asynchronous capsule.

20     The access network shall set the LastPacket bit of the Control Channel Header to ‘1’ for the  
21       Control Channel MAC Layer packet of an asynchronous capsule.

22     The access network shall set the Offset field of the Control Channel Header to ‘00’ for the  
23       Control Channel MAC Layer packet of an asynchronous capsule.

24      8.2.5.5.2 Access Terminal Requirements

25      8.2.5.5.2.1 Initial Acquisition

26     When the access terminal detects a Control Channel preamble and determines that the  
27       packet being transmitted is the first Control Channel MAC Layer packet of a synchronous  
28       capsule, it shall subtract Offset slots from the beginning of the half slot boundary at which  
29       the preamble was detected, and shall set the result to the beginning of the 16-slot frame  
30       and the beginning of the Control Channel Cycle.

31      8.2.5.5.2.2 Normal Operation

32     If the access terminal receives a Control Channel MAC Layer packet that has the  
33       LastPacket bit in the Control Channel header set to ‘0’, the access terminal shall continue  
34       monitoring the Control Channel for the Control Channel MAC Layer packets of the same  
35       capsule until it either does not receive a Control Channel MAC Layer Packet at the  
36       designated time or it receives a Control Channel MAC Layer packet with the LastPacket bit  
37       set to ‘1’.

1    8.2.5.5.2.3 Control Channel Supervision

2    Upon entering the active state, the access terminal shall set the Control Channel  
 3    supervision timer for  $T_{CCMPSupervision}$ . If a Control Channel capsule is received while the timer  
 4    is active, the timer is reset and restarted. If the timer expires the protocol returns a  
 5    *SupervisionFailed* indication and disables the timer.

6    8.2.5.5.2.4 Address Matching

7    When the access terminal receives a Control Channel MAC packet, it shall perform the  
 8    following:

- 9       • Access terminal shall parse the packet into its constituent Security Layer packets.
- 10      • Access terminal shall forward the Security Layer packet along with the  
 11       SecurityLayerFormat and the ConnectionLayerFormat fields to the Security Layer if  
 12       either of the following two conditions are met:
  - 13       – If the ATIType field and the ATI field of the ATI Record in the MAC Layer header of  
 14       a Security Layer packet is equal to the ATIType and ATI fields of any member of  
 15       the Address Management Protocol's ReceiveATIList.
  - 16       – If the ATIType of the ATI Record in the MAC Layer header of a Security Layer  
 17       packet is equal to '00' (i.e., BATI).
- 18      • Otherwise, the access terminal shall discard the Security Layer packet.

19    8.2.6 Header Formats

20    8.2.6.1 MAC Layer Header Format

21    The access network shall place the following header in front of every transmitted Security  
 22    Layer packet:

Field	Length (bits)
Length	8
SecurityLayerFormat	1
ConnectionLayerFormat	1
Reserved	4
ATI Record	2 or 34

23    Length                                  The access network shall set this field to the combined length, in  
 24    octets, of the Security Layer packet and this MAC Layer header  
 25    excluding the Length field.

26    SecurityLayerFormat

27    The access network shall set this field to '1' if security layer packet  
 28    has security applied; otherwise, the access network shall set this field  
 29    to '0'.

- 1 ConnectionLayerFormat  
 2                                  The access network shall set this field to '1' if the connection layer  
 3                                  packet is Format B; otherwise, the access network shall set this field  
 4                                  to '0'.  
 5 Reserved                        The access network shall set this field to all zeros. The access  
 6                                  terminal shall ignore this field.  
 7 ATI Record                      Access Terminal Identifier Record. The access network shall set this  
 8                                  field to the record specifying the access terminal's address. This  
 9                                  record is defined in 10.2.

10 8.2.6.2 Control Channel Header Format

11 The access network shall place the following header in front of every Control Channel MAC  
 12 Layer packet:

Field	Length (bits)
SynchronousCapsule	1
LastPacket	1
Offset	2
Reserved	4

- 13 SynchronousCapsule  
 14                                  For the first Control Channel MAC Layer packet of a synchronous  
 15                                  capsule, the access network shall set this field to '1'; otherwise, the  
 16                                  access network shall set this field to '0'.  
 17 LastPacket                     For the last Control Channel MAC Layer packet of a synchronous  
 18                                  capsule or asynchronous capsule, the access network shall set this  
 19                                  field to '1'; otherwise, the access network shall set this field to '0'.  
 20 Offset                         For the first Control Channel MAC Layer packet of a synchronous  
 21                                  capsule, the access network shall set this field to the offset in slots of  
 22                                  the Synchronous Control Channel relative to the Control Channel  
 23                                  Cycle; otherwise, the access network shall set this field to zero.  
 24 Reserved                      The access network shall set this field to zero. The access terminal  
 25                                  shall ignore this field.  
 26 8.2.6.3 Pad  
 27 The access network shall add sufficient padding so that the Control Channel MAC Layer  
 28                                  packet including all payload and headers is 1000 bits long.  
 29 The access network shall set the padding bits to '0'. The access terminal shall ignore the  
 30                                  padding bits.

- 1    8.2.6.4 Reserved  
 2    The access network shall add 2 reserved bits.  
 3    The access network shall set the reserved bits to '0'. The access terminal shall ignore the  
 4    reserved bits.

5    8.2.7 Protocol Numeric Constants

6

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
NCCMPType	Type field for this protocol	Table 2.3.6-1
NCCMPDefault	Subtype field for this protocol	0x0000
TCCMPSupervision	Control Channel supervision timer value	12 Control Channel Cycles

7    8.2.8 Interface to Other Protocols

8    8.2.8.1 Commands

9    This protocol does not issue any commands.

10   8.2.8.2 Indications

11   This protocol does not register to receive any indications.

12

### 8.3 Default Access Channel MAC Protocol

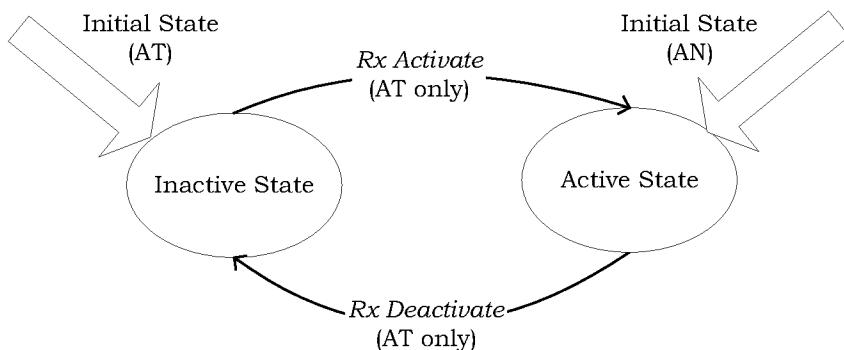
#### 8.3.1 Overview

The Default Access Channel MAC Protocol provides the procedures and messages required for an access terminal to transmit and an access network to receive the Access Channel.

This specification assumes that the access network has one instance of this protocol for all access terminals.

This protocol can be in one of two states:

- Inactive State: In this state the protocol waits for an *Activate* command. This state corresponds only to the access terminal and occurs when the access terminal has not acquired an access network or the access terminal has a connection open.
- Active State: In this state the access terminal transmits and the access network receives the Access Channel.



**Figure 8.3.1-1. Default Access Channel MAC Protocol State Diagram**

#### 8.3.2 Primitives and Public Data

##### 8.3.2.1 Commands

This protocol defines the following commands:

- *Activate*
- *Deactivate*

##### 8.3.2.2 Return Indications

This protocol returns the following indications:

- *TransmissionSuccessful*
- *TransmissionAborted*
- *TransmissionFailed*
- *TxStarted*

- *TxEnded*
- *SupervisionFailed*

### 8.3.2.3 Public Data

This protocol shall make the following data public:

- DataOffsetNom
- DataOffset9k6
- PowerStep
- OpenLoopAdjust
- ProbeInitialAdjust
- PreambleLength
- AccessSignature field of the next AccessParameters message that it will send
- MI<sub>ACMAC</sub>
- MQ<sub>ACMAC</sub>

### 8.3.3 Basic Protocol Numbers

The Type field for the Access Channel MAC Protocol is one octet, set to N<sub>ACMPType</sub>.

The Subtype field for the Default Access Channel MAC Protocol is two octets, set to N<sub>ACMPDefault</sub>.

### 8.3.4 Protocol Data Unit

The transmission unit of this protocol is the Access Channel MAC Layer packet. Each Access Channel MAC Layer packet contains part or all of a Security Layer packet.

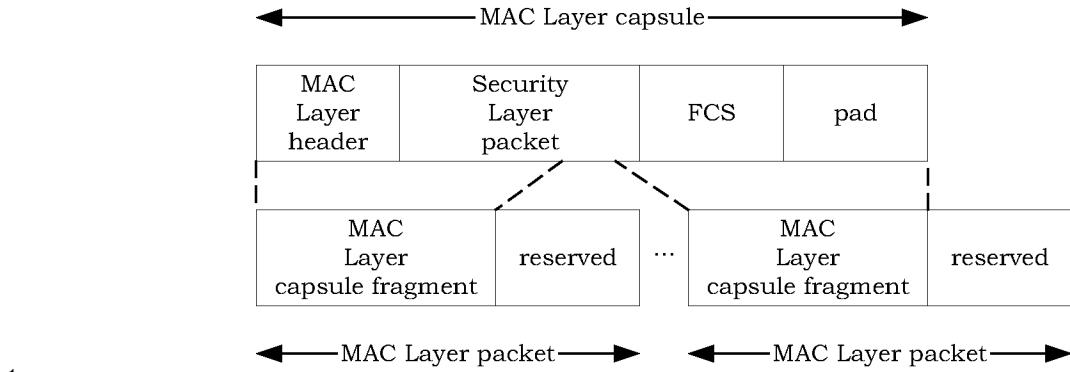
The protocol constructs one or more packets out of the Security Layer packet as follows:

- it adds the MAC Layer header specified in 8.3.6.1 in front of the Security Layer packet,
- it adds the FCS as defined in 8.3.6.2,
- it pads the Security Layer packet as defined in 8.3.6.3,
- it splits the result into one or more Access Channel MAC Layer capsule fragments,
- it adds the reserved bits, as defined in 8.3.6.4, to the capsule fragments to construct the Access Channel MAC Layer packets.

This protocol passes the packets for transmission to the Physical Layer. An example of the packet structure is shown in Figure 8.3.4-1.

Received packets are passed for further processing to the Security Layer after concatenation, removing the padding, FCS checking, and removing the MAC layer headers.

The value of the SecurityLayerFormat and ConnectionLayerFormat fields shall be passed to the Security Layer with the Security Layer packet.



**Figure 8.3.4-1. Access Channel MAC Packet Structure**

### 8.3.5 Procedures

#### 8.3.5.1 Protocol Initialization and Configuration

The access terminal shall start this protocol in the Inactive State.

The access network shall start this protocol in the Active State.

Access Channel parameters are provided by using the AccessParameters message, by using the ConfigurationRequest/ConfigurationResponse messages, or by using a protocol constant. Section 8.3.6.6 defines the AccessParameters message. Section 8.3.6.7.1.1 defines the complex attribute that can be configured and the default values the access terminal shall use unless superceded by a configuration exchange (see 10.3). Section 8.3.7 lists the protocol constants.

#### 8.3.5.2 Command Processing

The access network shall ignore all commands.

##### 8.3.5.2.1 Activate

If this protocol receives an *Activate* command in the Inactive State,

- The access terminal shall transition to the Active State.
- The access network shall ignore it.

If this protocol receives the command in the Active State it shall be ignored.

##### 8.3.5.2.2 Deactivate

If this protocol receives a *Deactivate* command in the Inactive State, it shall be ignored.

If this protocol receives the command in the Active State,

- The access terminal shall transition to the Inactive State.
- The access network shall ignore it.

1    8.3.5.3 Access Channel Structure

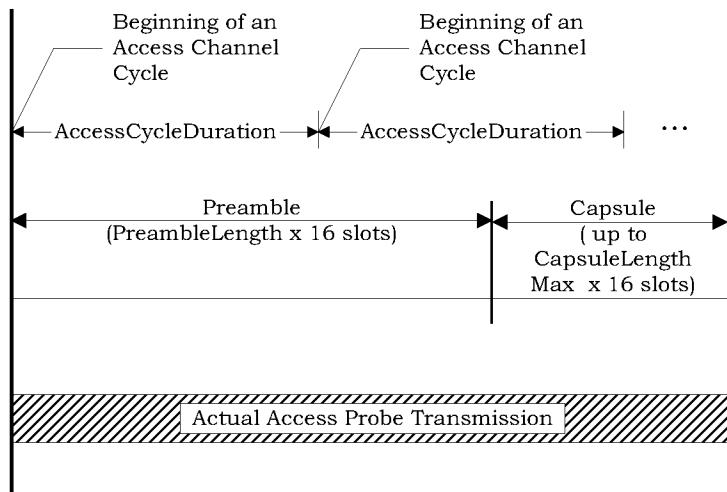
2    Figure 8.3.5.3-1 and Figure 8.3.5.3-2 illustrate the access probe structure and the access  
3    probe sequence.

4    The Access Channel Cycle specifies the time instants at which the access terminal may  
5    start an access probe. An Access Channel probe may only begin at times T such that

6               $T \bmod \text{AccessCycleDuration} = 0,$

7    where T is system time in slots.

8    The structure of an individual access probe is shown in Figure 8.3.5.3-1. In each access  
9    probe, the pilot (I-channel) is first enabled and functions as a preamble. After  
10   PreambleLength frames (PreambleLength  $\times$  16 slots), the probe data (Q-channel) is enabled  
11   for up to CapsuleLengthMax  $\times$  16 slots.



12              **Figure 8.3.5.3-1. Access Probe Structure**

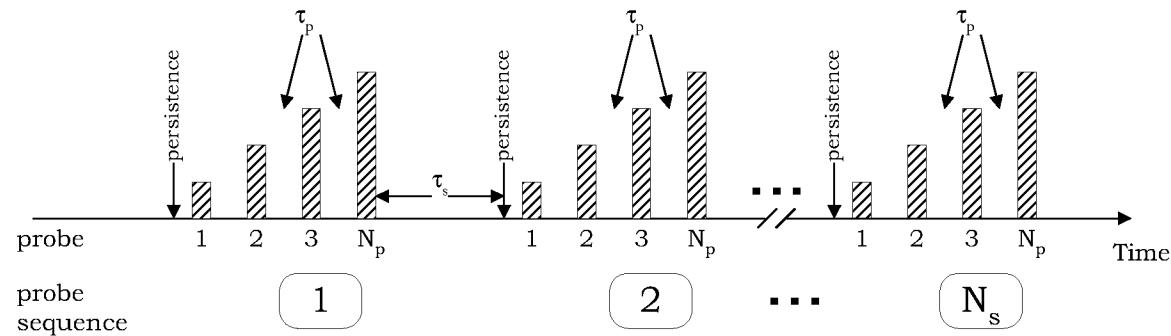
13    Each probe in a sequence is transmitted at increased power until any of the following  
14   conditions are met:

- 15         • Access terminal receives an ACAck message.
- 16         • Transmission is aborted because the protocol received a *Deactivate* command, or
- 17         • Maximum number of probes per sequence (ProbeNumStep) has been transmitted.

18    Prior to the transmission of the first probe, the access terminal performs a persistence test  
19   which is used to control congestion on the Access Channel.

20   Additionally the access terminal performs a persistence test in between probe sequences.

1



2

**Figure 8.3.5.3-2. Access Probe Sequences**

## 3 8.3.5.4 Inactive State

5 This state applies only to the access terminal.

6 In this state the access terminal waits for an *Activate* command.

## 7 8.3.5.5 Active State

8 In this state the access terminal is allowed to transmit on the Access Channel and the  
9 access network is monitoring the Access Channel.10 If the protocol receives a *Deactivate* command,

- 11 • Access terminal shall:
  - 12 – Immediately cease transmitting on the Access Channel if it is in the process of  
13 sending a probe.
  - 14 – Return a *TransmissionAborted* indication if it was in the process of sending an  
15 Access Channel MAC Layer packet.
  - 16 – Transition to the Inactive State.
- 17 • Access network shall ignore this command.

18 All other commands shall be ignored in this state.

## 19 8.3.5.5.1 Access Terminal Requirements

20 This protocol enforces a stop and wait packet transmission policy over the Access Channel.  
21 That is, the access terminal shall not send a new Access Channel MAC Layer packet before  
22 either:

- 23 • Receipt of an ACAck message for the previous packet, or
- 24 • transmission of the previous packet failed after transmitting *ProbeSequenceMax*  
25 probe sequences for it.

1 The access terminal shall return a *TxStarted* indication before transmitting the first probe  
 2 for an Access Channel MAC Layer packet.<sup>39</sup>

3 The access terminal shall return a *TxEnded* indication either:

- 4 • Simultaneous with a *TransmissionAborted* or a *TransmissionFailed* indication, or
- 5 •  $T_{ACMPTransaction}$  seconds after a *TransmissionSuccessful* indication.

6 8.3.5.5.1.1 Probe Transmission

7 The access terminal shall conform to the following rules when sending a probe:

- 8 1. **Current SectorParameters**. The access terminal shall verify that the value of  
 9 SectorSignature field of the latest QuickConfig message is the same as  
 10 SectorSignature field of the latest SectorParameters message prior to sending the  
 11 first probe of the first probe sequence. Both SectorSignature values (one belonging  
 12 to the QuickConfig message and one belonging to the SectorParameters message are  
 13 public data of the Overhead Messages Protocol).
- 14 2. **Current AccessParameters**. Prior to sending the first probe of the probe sequence,  
 15 the access terminal shall verify that the last AccessParameters message it received is  
 16 current, according to the last AccessSignature value given as public data by the  
 17 Overhead Messages Protocol. If the AccessParameters message is not current, the  
 18 access terminal shall start the AccessParameters supervision timer for  
 19  $T_{ACMPASSupervision}$ . If the timer expires before it receives the current AccessParameters  
 20 message, the access terminal shall return a *SupervisionFailed* indication and  
 21 transition to the Inactive State.
- 22 3. **ATI Record**. The access terminal shall set the ATI and ATIType fields of the ATI  
 23 Record in the MAC Layer header to *TransmitATI.ATI* and *TransmitATI.ATIType*,  
 24 respectively (*TransmitATI* is provided as public data by the Address Management  
 25 Protocol).
- 26 4. **Probe Power Control**. The access terminal shall send the  $i$ -th probe in the probe  
 27 sequence at a power level given by  $X_0 + (i-1) \times PowerStep$ , where  $X_0$  represents the  
 28 access terminal's open-loop mean output power of the Pilot Channel and is given by  
 29 
$$X_0 = - \text{Mean Rx Power (dBm)} + \text{OpenLoopAdjust} + \text{ProbeInitialAdjust}$$
  
 30 and the Mean Rx Power is estimated throughout the transmission of each probe.
- 31 5. **Probe Structure**. When sending a probe, the access terminal shall transmit  
 32 PreambleLength frames of pilot only, followed by up to CapsuleLengthMax frames of  
 33 probe data and pilot. The access terminal shall transmit a single Access Channel  
 34 Capsule per probe. The access terminal shall not change the probe data contents in  
 35 between probes.

---

<sup>39</sup> Higher layer protocols use this indication as a notification that there may be an outstanding transaction on the Access Channel; and, therefore, the access terminal should not go to sleep.

6. Long Code Cover. The access terminal shall use the Access Channel long codes to cover the entire probe. The Access Channel long code is specified in 8.3.5.5.1.2.
  7. Inter-Probe Backoff. After sending an access probe within an access probe sequence, the access terminal shall wait for  $\tau_p$  slots after the end of the access probe before sending the next probe in a probe sequence, where  $\tau_p = T_{ACMPATProbeTimeout} + (y \times AccessCycleDuration)$  and  $y$  is a uniformly distributed integer random number between 0 and ProbeBackoff. The access terminal shall not send the next probe in this probe sequence if it receives an ACAck message or it has already transmitted ProbeNumStep ( $N_p$  in Figure 8.3.5.3-2) probes in this probe sequence.

#### 8.3.5.5.1.2 Access Channel Long Code Masks

The access terminal shall set the Access Channel long masks,  $MI_{ACMAC}$  and  $MQ_{ACMAC}$  as follows.

The 42-bit masks  $\text{MIACMAC}$  and  $\text{MQACMAC}$  are specified in Table 8.3.5.5.1.2-1.

**Table 8.3.5.5.1.2-1. Access Channel Long Code Masks**

In Table 8.3.5.5.1.2-1:

- SectorID is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe.
  - ColorCode is given as public data of Overhead Messages Protocol and corresponds to the sector to which the access terminal is sending the access probe.
  - AccessCycleNumber is defined as follows:

AccessCycleNumber = SystemTime mod 256

Where:

SystemTime is the CDMA System Time in slots corresponding to the slot in which the first access probe preamble for this access probe is sent. System Time is given as public data of Initialization State Protocol, and

`Permuted(ColorCode | SectorID[23:0])'` and `AccessCycleNumber'` are bitwise complement of `Permuted(ColorCode | SectorID[23:0])` and `AccessCycleNumber`, respectively. `Permuted(ColorCode | SectorID[23:0])` is a permutation of the bits in `ColorCode | SectorID[23:0]` and is defined as follows:

ColorCode | SectorID[23:0] = (S<sub>31</sub>, S<sub>30</sub>, S<sub>29</sub>, ..., S<sub>0</sub>)

Permuted(ColorCode | SectorID[23:0]) =

$(S_0, S_{31}, S_{22}, S_{13}, S_4, S_{26}, S_{17}, S_8, S_{30}, S_{21}, S_{12}, S_3, S_{25}, S_{16}, S_7, S_{29}, S_{20}, S_{11}, S_2, S_{24}, S_{15}, S_6, S_{28}, S_{19}, S_{10}, S_1, S_{23}, S_{14}, S_5, S_{27}, S_{18}, S_9)$ .

1        8.3.5.5.1.3 Probe Sequence Transmission

2        The access terminal shall conform to the following rules when sending a probe sequence:

- 3        1. **Persistence Test.** Prior to sending the first probe of the sequence, the access  
 4        terminal shall perform a persistence test in each Access Channel Cycle. For this  
 5        test, the access terminal shall use the value  $p$  as specified by APersistence[ $i$ ] where  $i$   
 6        is the class of the access terminal and APersistence[ $i$ ] is the  $(i+1)^{\text{st}}$  occurrence of the  
 7        APersistence field in the AccessParameters message.<sup>40</sup> If the access terminal does  
 8        not have a class defined, it shall use  $i=0$ , corresponding to non-emergency access  
 9        terminals.

10      When  $p$  is not zero, the persistence test consists of comparing a uniformly  
 11     distributed random number  $x$ ,  $0 < x < 1$ , with  $p$ . If  $x < p$  the test is said to succeed.  
 12     If the persistence test succeeds or if the number of consecutive unsuccessful  
 13     persistence tests exceeds  $4/p$ , the access terminal may transmit in this Access  
 14     Channel Cycle. Otherwise, if  $p$  is not equal to zero, the access terminal shall repeat  
 15     the persistence test in the next Access Channel Cycle. If  $p$  is equal to zero, the  
 16     access terminal shall return a *TransmissionFailure* indication and end the access.

- 17      2. **Transmitter Power.** The access terminal shall not transmit a probe if it cannot  
 18     transmit the probe at the prescribed power. If the access terminal does not transmit  
 19     a probe for this reason, it shall abort the probe sequence. Aborted probe sequences  
 20     are counted as part of the total ProbeSequenceMax probe sequences the access  
 21     terminal is allowed to transmit for a given access.
- 22      3. **Probe Contents.** The access terminal shall not change the data portion of the probe  
 23     contents between probe sequences.
- 24      4. **Success Condition.** If the access terminal receives an ACAck message it shall stop  
 25     the probe sequence, including any transmission in progress, and shall return a  
 26     *TransmissionSuccessful* indication.
- 27      5. **Failure Condition.** If the access terminal has already sent ProbeSequenceMax probe  
 28     sequences for this access (Ns in Figure 8.3.5.3-2), and if it does not receive an  
 29     ACAck message acknowledging its receipt within  $(T_{ACMPATProbeTimeout} + T_{ACMPCycleLen})$   
 30     slots after the end of the last access probe, the access terminal shall return a  
 31     *TransmissionFailed* indication and abort the access.
- 32      6. **Inter-Sequence Backoff.** The access terminal shall generate a uniformly distributed  
 33     integer random number  $k$  between 0 and ProbeSequenceBackoff. The access  
 34     terminal shall wait for  $\tau_s = (k \times \text{AccessCycleDuration}) + T_{ACMPATProbeTimeout}$  slots from  
 35     the end of the last probe of the previous sequence before repeating this sequence.

---

40 The access terminal's class is configured through means that are outside the scope of this specification.

#### 8.3.5.5.2 Access Network Requirements

2 The access network should send an AccessParameters message at least once every  
3  $N_{ACMPAccessParameters}$  slots.

4 The access network should send an ACAck message in response to every Access Channel  
5 MAC Layer capsule it receives. The message should be sent within  $T_{ACMPANProbeTimeout}$  slots of  
6 receipt of the packet.

7 The access network should monitor and control the load on the Access Channel. The access  
8 network may control the load by adjusting the access persistence vector, APersistence, sent  
9 as part of the AccessParameters message.

### 10 8.3.6 Header and Message Formats

### 11 8.3.6.1 MAC Layer Header

12 The access terminal shall place the following header in front of the Security Layer packet:

Field	Length (bits)
Length	8
SessionConfigurationToken	16
SecurityLayerFormat	1
ConnectionLayerFormat	1
Reserved	4
ATI Record	34

## 17 SessionConfigurationToken

18 The access terminal shall set this field to the value of the  
19 SessionConfigurationToken which is public data of the Session  
20 Configuration Protocol.

## 21 SecurityLayerFormat

22 The access terminal shall set this field to '1' if security layer packet  
23 has security applied; otherwise, the access terminal shall set this  
24 field to '0'.

## 25 ConnectionLayerFormat

26 The access terminal shall set this field to ‘1’ if the connection layer  
27 packet is Format B; otherwise, the access terminal shall set this field  
28 to ‘0’.

1	Reserved	The access terminal shall set this field to zero. The access network shall ignore this field.
2		
3	ATI Record	Access Terminal Identifier Record. The access terminal shall set this field to the record specifying the access terminal's ID specified by TransmitATI.ATI and TransmitATI.ATIType. This record is defined in 10.2.
4		
5		
6		

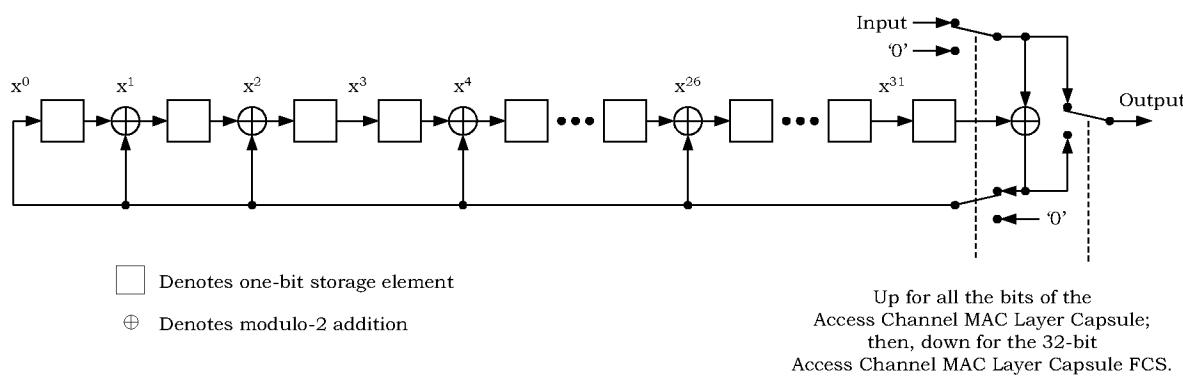
### 8.3.6.2 FCS

The FCS shall be calculated using the standard CRC-CCITT generator polynomial:

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1$$

The FCS shall be equal to the value computed by the following procedure and the logic shown below:

- All shift register elements shall be initialized to logical zeros.
- Switches shall be set in the up position.
- Register shall be clocked once for each bit of Access Channel MAC Layer Capsule, excluding the FCS and padding bits. The Access Channel MAC Layer Capsule is read in order from MSB to LSB, starting with the MSB of the MAC Layer header
- Switches shall be set in the down position so that the output is a modulo-2 addition with a '0' and the successive shift register inputs are '0'.
- Register shall be clocked an additional 32 times for the 32 FCS bits.



**Figure 8.3.6.2-1. Access Channel MAC Layer Capsule FCS**

### 8.3.6.3 Padding Bits

The access terminal shall add sufficient padding so that the Access Channel MAC capsule, including all payload, FCS, padding, and headers, is the smallest possible integer multiple of 232 bits. The access terminal shall set the padding bits to '0'. The access network shall ignore the padding bits.

## 1    8.3.6.4 Reserved Bits

2    The access terminal shall add 2 reserved bits to each Access Channel capsule fragment.

3    The access terminal shall set the reserved bits to '0'. The access network shall ignore the  
4    reserved bits.

## 5    8.3.6.5 ACAck

6    The access network sends the ACAck message to acknowledge receipt of an Access Channel  
7    MAC Layer capsule.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8

8    MessageID         The access network shall set this field to 0x00.

<b>Channels</b>	CC	<b>SLP</b>	Best Effort
<b>Addressing</b>	unicast	<b>Priority</b>	10

## 10    8.3.6.6 AccessParameters

11    The AccessParameters message is used to convey Access Channel information to the access  
12    terminals.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
AccessCycleDuration	8
AccessSignature	16
OpenLoopAdjust	8
ProbeInitialAdjust	5
ProbeNumStep	4
PreambleLength	3

13     $N_{ACMPAPersist}$  occurrences of the following field:

APersistence	6
--------------	---

Reserved	variable
----------	----------

14    MessageID         The access network shall set this field to 0x01.

15    AccessCycleDuration

16    The access network shall set this field to the duration of an Access  
17    Channel Cycle in units of slots.

1	AccessSignature	AccessParameters message signature. The access network shall change this field if the contents of the AccessParameters message change.
4	OpenLoopAdjust	The access network shall set this field to the negative of the nominal power to be used by access terminals in the open loop power estimate, expressed as an unsigned value in units of 1 dB.
7	ProbeInitialAdjust	The access network shall set this field to the correction factor to be used by access terminals in the open loop power estimate for the initial transmission on the Access Channel, expressed as a two's complement value in units of 1 dB.
11	ProbeNumStep	The access network shall set this field to the maximum number of access probes access terminals are to transmit in a single access probe sequence. The access network shall set this field to a value in the range [1 ... 15].
15	PreambleLength	The access network shall set this field to the length in frames of the access probe preamble.
17	APersistence	Access persistence vector. If a value in this vector is 0x3F, the access terminal shall use zero as the corresponding persistence probability; otherwise, if the value of this field, $n$ , not equal to 0x3F, the access terminal shall use $2^{n/4}$ as the corresponding persistence probability.
21	Reserved	Number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

<b>Channels</b>	CC	<b>SLP</b>	Best Effort
<b>Addressing</b>	Broadcast	<b>Priority</b>	30

### 25 8.3.6.7 Configuration Messages

26 The Default Access Channel MAC Protocol uses the Generic Configuration Protocol to  
27 transmit configuration parameters from the access network to the access terminal.

## 1    8.3.6.7.1 Configurable Attributes

2    8.3.6.7.1.1 The following complex attributes and default values are defined (see  
 3                          10.3):InitialConfiguration

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
CapsuleLengthMax	4	2
PowerStep	4	6
ProbeSequenceMax	4	3
ProbeBackoff	4	4
ProbeSequenceBackoff	4	8
Reserved	4	N/A

- 5    Length                         Length of the complex attribute in octets. The access network shall  
 6                                     set this field to the length of the complex attribute excluding the  
 7                                     Length field.
- 8    AttributeID                 Parameter set identifier. The access network shall set this field to  
 9                                     0x00.
- 10   ValueID                         The access network shall set this field to an identifier assigned to this  
 11                                     complex attribute. The access network should change this field for  
 12                                     each set of values for this complex attribute.
- 13   CapsuleLengthMax             Access Channel Capsule length. The access network shall set this  
 14                                     field to the maximum number of frames in an Access Channel  
 15                                     Capsule. The access terminal shall support all the valid values  
 16                                     specified by this field.
- 17   PowerStep                         Probe power increase step. The access network shall set this field to  
 18                                     the increase in power between probes, in resolution of 0.5 dB. The  
 19                                     access terminal shall support all the valid values specified by this  
 20                                     field.
- 21   ProbeSequenceMax             Maximum number of probe sequences. The access network shall set  
 22                                     this field to the maximum number of probe sequences for a single  
 23                                     access attempt. The access terminal shall support all the valid values  
 24                                     specified by this field.

- |    |                      |   |
|----|----------------------|---|
| 1  | ProbeBackoff         | Inter-probe backoff. The access network shall set this field to the upper limit of the backoff range (in units of AccessCycleDuration) that the access terminal is to use between probes. The access terminal shall support all the valid values specified by this field.                   |
| 2  | ProbeSequenceBackoff | Inter-probe sequence backoff. The access network shall set this field to the upper limit of the backoff range (in units of AccessCycleDuration) that the access terminal is to use between probe sequences. The access terminal shall support all the valid values specified by this field. |
| 3  | Reserved             | The access network shall set this field to zero. The access terminal shall ignore this field.   |
| 4  |                      |   |
| 5  |                      |   |
| 6  |                      |   |
| 7  |                      |   |
| 8  |                      |   |
| 9  |                      |   |
| 10 |                      |   |
| 11 |                      |   |
| 12 |                      |   |

#### 8.3.6.7.1.2 PowerParameters Attribute

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
DataOffsetNom	4	0
DataOffset9k6	4	0

- |    |               |  |
|----|---------------|--|
| 15 | Length        | Length of the complex attribute in octets. The access network shall set this field to the length of the complex attribute excluding the Length field.  |
| 16 |               |  |
| 17 |               |  |
| 18 | AttributeID   | The access network shall set this field to 0x01.   |
| 19 | ValueID       | The access network shall set this field to an identifier assigned to this complex value.   |
| 20 |               |  |
| 21 | DataOffsetNom | The access network shall set this field to the nominal offset of the access data channel power to pilot channel power, expressed as 2's complement value in units of 0.5 dB. The access terminal shall support all the valid values specified by this field.               |
| 22 |               |  |
| 23 |               |  |
| 24 |               |  |
| 25 | DataOffset9k6 | The access network shall set this field to the ratio of access channel power at 9600 bps to the nominal access channel power at 9600 bps, expressed as 2's complement in units of 0.25 dB. The access terminal shall support all the valid values specified by this field. |
| 26 |               |  |
| 27 |               |  |
| 28 |               |  |

1    8.3.6.7.2 ConfigurationRequest

2    The ConfigurationRequest message format is given as part of the Generic Configuration  
3    Protocol (see 10.7).

4    The MessageID field for this message shall be set to 0x50.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

6    8.3.6.7.3 ConfigurationResponse

7    The ConfigurationResponse message format is given as part of the Generic Configuration  
8    Protocol (see 10.7).

9    The MessageID field for this message shall be set to 0x51.

10   If the access terminal includes an attribute with this message, it shall set the AttributeID  
11   field of the message to the AttributeID field of the ConfigurationRequest message associated  
12   with this response and it shall set the ValueID field to the ValueID field of one of the  
13   complex attribute values offered by the ConfigurationRequest message.

14

<b>Channels</b>	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

1      8.3.7 Protocol Numeric Constants

2

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>ACMPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>ACMPDefault</sub>	Subtype field for this protocol	0x0000
N <sub>ACMPAPersist</sub>	Number of different persistence values	4
N <sub>ACMPAccessParameters</sub>	The recommended maximum number of slots between transmission of two consecutive AccessParameters message.	3 * T <sub>ACMPCycleLen</sub>
T <sub>ACMPAPSupervision</sub>	AccessParameters supervision timer	12 * T <sub>ACMPCycleLen</sub>
T <sub>ACMPATProbeTimeout</sub>	Time to receive an acknowledgment at the access terminal for a probe before sending another probe	128 slots
T <sub>ACMPANProbeTimeout</sub>	Maximum time to send an acknowledgment for a probe at the access network	96 slots
T <sub>ACMPTransaction</sub>	Time for access terminal to wait after a successful transmission before returning a <i>TxEnded</i> indication	1 second
T <sub>ACMPCycleLen</sub>	Length of Control Channel Cycle	256 slots

3      8.3.8 Interface to Other Protocols

4      8.3.8.1 Commands

5      This protocol does not issue any commands.

6      8.3.8.2 Indications

7      This protocol does not register to receive any indications.

8

## 1    8.4 Default Forward Traffic Channel MAC Protocol

### 2    8.4.1 Overview

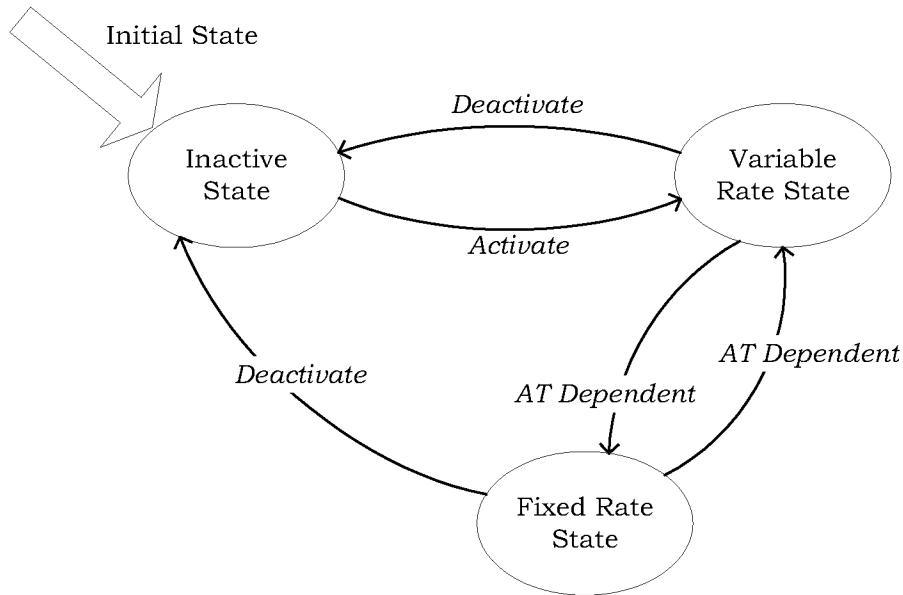
3    The Default Forward Traffic Channel MAC Protocol provides the procedures and messages  
 4    required for an access network to transmit and an access terminal to receive the Forward  
 5    Traffic Channel. Specifically, this protocol addresses Forward Traffic Channel addressing  
 6    and Forward Traffic Channel rate control.

7    The access network maintains an instance of this protocol for every access terminal.

8    This protocol operates in one of three states:

- 9    • Inactive State: In this state, the access terminal is not assigned a Forward Traffic  
 10   Channel. When the protocol is in this state, it waits for an *Activate* command.
- 11   • Variable Rate State: In this state, the access network transmits the Forward Traffic  
 12   Channel at a variable rate, as a function of the access terminal's DRC value.
- 13   • Fixed Rate State: In this state, the access network transmits the Forward Traffic  
 14   Channel to the access terminal from one particular sector, at one particular rate.

15   The protocol states and allowed transitions between the states are shown in Figure 8.4.1-1.  
 16   The rules governing these transitions are provided in sections 8.4.5.1, 8.4.5.4, 8.4.5.5.2,  
 17   and 8.4.5.6.3 for transitions out of the Inactive State, Variable Rate State, and Fixed Rate  
 18   State.



19   **Figure 8.4.1-1. Forward Traffic Channel MAC Protocol State Diagram**

1    8.4.2 Primitives and Public Data

2    8.4.2.1 Commands

3    This protocol defines the following commands:

- 4       • *Activate*

- 5       • *Deactivate*

6    8.4.2.2 Return Indications

7    This protocol returns the following indications:

- 8       • *SupervisionFailed*

9    8.4.2.3 Public Data

10   This protocol shall make the following data public:

- 11      • DRCGating

- 12      • DRCLength

- 13      • DRCChannelGain

- 14      • AckChannelGain

- 15      • DRCCover for every pilot in the Active Set

- 16      • Transmission rate in the Fixed Rate State

17   8.4.3 Basic Protocol Numbers

- 18      • Type field for this protocol is one octet, set to N<sub>FTCMPType</sub>

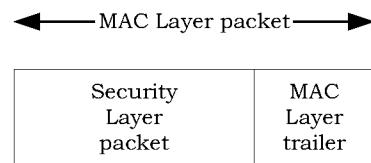
- 19      • Subtype field for this protocol is two octets, set to N<sub>FTCMPDefault</sub>

20   8.4.4 Protocol Data Unit

21   The transmission unit of this protocol is a Forward Traffic Channel MAC Layer packet. Each  
22   packet consists of one Security Layer packet.

23   The protocol constructs a Forward Traffic Channel MAC Layer packet out of the Security  
24   Layer packet by adding the MAC Layer trailer as defined in 8.4.6.1.

25   The protocol then sends the packet for transmission to the Physical Layer. The packet  
26   structure is shown in Figure 8.4.4-1.



27  
28   **Figure 8.4.4-1. Forward Traffic Channel MAC Layer Packet Structure**

1 If the MACLayerFormat field of the MAC Layer trailer is equal to '1', received packets are  
2 passed for further processing to the Security Layer after removing the layer-related trailer.  
3 The access terminal shall discard the MAC packet if the MACLayerFormat field of the MAC  
4 Layer trailer is equal to '0'. The ConnectionLayerFormat field within the MAC Layer trailer  
5 shall be passed to the Security Layer with the Security Layer packet.

6 8.4.5 Procedures

7 8.4.5.1 Protocol Initialization and Configuration

8 This protocol shall be started in the Inactive State.

9 The parameters for the Default Forward Traffic Channel MAC protocol are provided by  
10 using the ConfigurationRequest/ConfigurationResponse messages or by using a protocol  
11 constant. Section 8.4.6.4 defines the attributes that can be configured and the default  
12 values that the access terminal shall use unless superseded by a configuration exchange.  
13 Section 8.4.7 lists the protocol constants.

14 8.4.5.2 Command Processing

15 8.4.5.2.1 Activate

16 If this protocol receives an *Activate* command in the Inactive State, the access terminal and  
17 the access network shall transition to the Variable Rate State.

18 If this protocol receives the command in any other state it shall be ignored.

19 8.4.5.2.2 Deactivate

20 If the protocol receives a *Deactivate* command in the Variable Rate State or the Fixed Rate  
21 State,

- 22 • The access terminal shall cease monitoring the Forward Traffic Channel, shall cease  
23 transmitting the DRC Channel, and shall transition to the Inactive State.
- 24 • The access network should cease transmitting the Forward Traffic Channel to this  
25 access terminal, should cease receiving the DRC channel from this access terminal,  
26 and should transition to the Inactive State.

27 If this command is received in the Inactive State it shall be ignored.

28 8.4.5.3 Forward Traffic Channel Addressing

29 Transmission on the Forward Traffic Channel is time division multiplexed. At any given  
30 time, the channel is either being transmitted or not; and, if it is being transmitted, it is  
31 addressed to a single user. When transmitting the Forward Traffic Channel, the access  
32 network uses the MACIndex to identify the target access terminal.

33 Requirements for Forward Traffic Channel addressing are part of the Physical Layer.

1    8.4.5.4 Inactive State

2    When the protocol is in the Inactive State, the access terminal and the access network wait  
 3    for an *Activate* command.

4    8.4.5.5 Variable Rate State

5    In the Variable Rate State, the access network transmits at the rate dictated by the Data  
 6    Rate Control (DRC) Channel transmitted by the access terminal. The access terminal shall  
 7    use either a DRC cover index 0 or the DRC Cover index associated with a sector in its Active  
 8    Set. The DRC cover index 0 is called the “null cover”. A DRC cover that corresponds to a  
 9    sector in the access terminal’s Active Set is called a “sector cover”. The access terminal is  
 10   said to be pointing the DRC at a sector in its Active Set if the access terminal is using the  
 11   DRC cover corresponding to that sector.

12   The access terminal shall perform the supervision procedures described in 8.4.5.7 in the  
 13   Variable Rate State.

14   8.4.5.5.1 DRC and Packet Transmission Requirements

15   The access terminal uses the DRC cover to specify the transmitting sector (the access  
 16   terminal is said to point the DRC at that sector). The access terminal uses the DRC value to  
 17   specify the requested transmission rate.

18   8.4.5.5.1.1 Access Terminal Requirements

19   The access terminal shall obey the following rules when transmitting the DRC:

- 20   • access terminal shall use DRCLength slots to send a single DRC.
- 21   • The DRC value and/or cover may change in slots T such that:

$$22 \quad (T + 1 - \text{FrameOffset}) \bmod \text{DRCLength} = 0$$

23   where T is the system time in slots.

- 24   • If the DRCGating is equal to 1, the access terminal shall transmit the DRC over a one  
 25   slot period, starting in slot T that satisfies the following equation:

$$26 \quad (T + 2 - \text{FrameOffset}) \bmod \text{DRCLength} = 0$$

- 27   • DRC cover shall obey the following rules:

- 28   – If the access terminal’s current DRC cover is a sector cover, then the access  
 29   terminal’s next DRC cover shall not be a different sector cover. It may only be the  
 30   same sector cover or a null cover.

- 31   – If the access terminal’s most recent sector cover corresponds to sector A, then the access  
 32   terminal shall not use a sector cover corresponding to a sector B until the  
 33   access terminal has determined that packets received from sector B will not  
 34   overlap in time with packets received from sector A.

- 35   – The access terminal may inhibit reception of data from the access network by  
 36   covering the DRC with the null cover. The access terminal shall set the DRC to the  
 37   value it would have used had it requested data from the best serving sector.

- 1           – The access terminal shall use either the null cover or a sector cover (see 8.4.5.5)  
 2           as DRC cover.
- 3       • Access terminal shall set the DRC to one of the valid values in Table 8.4.5.5.1.1-1,  
 4           corresponding to the rate it requests.
- 5       • Access terminal shall set the DRC to the maximum value that channel conditions  
 6           permit for the sector at which the access terminal is pointing its DRC. The access  
 7           terminal uses the null rate if the channel conditions do not permit even the lowest  
 8           non-null rate.

9           **Table 8.4.5.5.1.1-1. DRC Value Specification**

DRC value	Rate (kbps)	Packet Length (Slots)
0x0	null rate	N/A
0x1	38.4	16
0x2	76.8	8
0x3	153.6	4
0x4	307.2	2
0x5	307.2	4
0x6	614.4	1
0x7	614.4	2
0x8	921.6	2
0x9	1228.8	1
0xa	1228.8	2
0xb	1843.2	1
0xc	2457.6	1
0xd	Invalid	N/A
0xe	Invalid	N/A
0xf	Invalid	N/A

- 10       • If the access terminal has finished sending its DRC to sector A during slot  $n$   
 11           specifying a requested rate  $r$ , the access terminal should search for a preamble  
 12           transmitted at rate  $r$  from sector A during slots  $n + 1$  through  $n + \text{DRCLength}$ .
- 13       • If the access terminal detects a preamble from any sector, the access terminal shall  
 14           continue to receive the entire packet from that sector, using the requested rate.
- 15       • If the access terminal is not already receiving a packet, it shall attempt to receive a  
 16           packet transmitted at the rate it requested through the corresponding DRC value.

- 1     • If the access terminal receives a DRCLock bit that is set to ‘0’ from the sector to  
 2        which it is pointing its DRC, the access terminal should stop pointing its DRC at that  
 3        sector.

4     8.4.5.5.1.2 Access Network Requirements

5     The access network shall obey the following rules when processing the DRC and sending a  
 6        packet to the access terminal:

- 7        • If the access network begins transmitting a packet to the access terminal at slot T, it  
 8        shall do so at the rate specified by the DRC whose reception was completed in slot  
 9         $T - 1 - ((T - \text{FrameOffset}) \bmod \text{DRCLength})$ .  
 10      • Once the access network initiates a packet transmission to a particular access  
 11        terminal, it shall continue transmitting to that access terminal until it receives a  
 12        *PhysicalLayer.ForwardTrafficCompleted* indication.

13     8.4.5.5.2 Transitions from the Variable Rate State

14     The access terminal may transition to the Fixed Rate State at any time. The access terminal  
 15        shall perform the following steps in order to transition to the Fixed Rate State.

- 16        • If the access terminal’s last sector cover was sector A, then the access terminal shall  
 17        continue using sector A’s cover until it has determined that it is no longer going to be  
 18        served by Sector A.  
 19        • Then, the access terminal shall cover the DRC with the null cover.  
 20        • Then, the access terminal shall send the *FixedModeRequest* message specifying:  
 21            – A sector in the active set.  
 22            – A data rate.

23     8.4.5.6 Fixed Rate State

24     In the Fixed Rate State, the access terminal receives Forward Traffic Channel MAC Layer  
 25        packets at a specific rate from a specific sector. When the access network transmits a  
 26        Forward Traffic Channel MAC Layer packet to the access terminal, it uses the specified  
 27        sector at the specified rate.

28     The access network shall perform at least one of the following actions within  $T_{\text{FTCMPANFixedMode}}$   
 29        seconds of entering the Fixed Rate State:

- 30        • Transmit a packet to the access terminal on the Forward Traffic Channel, or  
 31        • Send a *FixedModeResponse* message to the access terminal, specifying the  
 32        TransactionID of the last *FixedModeRequest* message it received.

33     Upon entering the Fixed Rate State, the access terminal shall set a transition timer for  
 34         $T_{\text{FTCPATFixedMode}}$  seconds.

35     If the transition timer is enabled and the access terminal receives a *FixedModeResponse*  
 36        message or a valid packet on the Forward Traffic Channel, the access terminal shall disable  
 37        this timer.

1 If the transition timer expires, the access terminal shall transition to the Variable Rate  
2 State by covering its DRC with a sector cover (see 8.4.5.6.3). The term “sector cover” is  
3 defined in 8.4.5.5.

4 The access terminal shall perform the supervision procedures described in 8.4.5.7 in the  
5 Fixed Rate State.

6 8.4.5.6.1 DRC Requirements

7 The access terminal shall cover the DRC with the null cover. The null cover is defined in  
8 8.4.5.5.

9 The access terminal shall set the DRC value to the value it would have requested from this  
10 serving sector, had it been in the Variable Rate State.

11 8.4.5.6.2 Packet Transmission

12 The access network shall only schedule Forward Traffic Channel MAC Layer packet  
13 transmissions to the access terminal on the Forward Traffic Channel transmitted by the  
14 sector specified in the FixedModeRequest message. The access network shall send the  
15 packet at the rate specified in the FixedModeRequest message. If the access network begins  
16 a packet transmission, it shall continue transmitting the packet until it receives a  
17 *PhysicalLayer.ForwardTrafficCompleted* indication. The access terminal shall monitor the  
18 Forward Traffic Channel transmitted by the sector specified in the FixedModeRequest  
19 message.

20 8.4.5.6.3 Transitions from the Fixed Rate State

21 In order to transition to the Variable Rate State, the access terminal shall cover its DRC  
22 with a sector cover. The access terminal shall transition to the Variable Rate State if the  
23 sector specified in the FixedModeRequest message is no longer a member of the access  
24 terminal’s Active Set.

25 8.4.5.7 Supervision Procedures

26 8.4.5.7.1 DRC Supervision

27 The access terminal shall perform supervision on the DRC as follows:

- 28 • The access terminal shall set the DRC supervision timer for  $T_{FTCMDRCSupervision}$  when it  
29 transmits a null rate DRC.
- 30 • If the access terminal requests a non-null rate while the DRC supervision timer is  
31 active, the access terminal shall disable the timer.
- 32 • If the DRC supervision timer expires, the access terminal shall disable the Reverse  
33 Traffic Channel transmitter and set the Reverse Traffic Channel Restart timer for  
34 time  $T_{FTCMPRestartTx}$ .
- 35 • If the access terminal generates consecutive non-null rate DRC values for more than  
36  $N_{FTCMPRestartTx}$  slots, the access terminal shall disable the Reverse Traffic Channel  
37 Restart timer and shall enable the Reverse Traffic Channel transmitter.

- 1     • If the Reverse Traffic Channel Restart timer expires, the access terminal shall return  
 2        a *SupervisionFailed* indication and transition to the Inactive State.

3     8.4.5.7.2 ForwardTrafficValid Monitoring

4     The access terminal shall monitor the bit associated with its MACIndex in the  
 5        ForwardTrafficValid field made available by the Overhead Messages protocol. If this bit is  
 6        set to 0, the access terminal shall return a *SupervisionFailed* indication and transition to  
 7        the Inactive State.

8     8.4.6 Trailer and Message Formats

9        8.4.6.1 MAC Layer Trailer

10      The access network shall set the MAC Layer Trailer as follows:

Field	Length (bits)
ConnectionLayerFormat	1
MACLayerFormat	1

12      ConnectionLayerFormat

13        The access network shall set this field to ‘1’ if the connection layer  
 14        packet is Format B; otherwise, the access network shall set this field  
 15        to ‘0’.

16      MACLayerFormat

17        The access network shall set this field to ‘1’ if the MAC layer packet  
 18        contains a valid payload; otherwise, the access network shall set this  
 19        field to ‘0’.

## 1    8.4.6.2 FixedModeRequest

2    The access terminal sends the FixedModeRequest message to indicate a transition to the  
 3    Fixed Rate State.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
TransactionID	8
DRCCover	3
RequestedRate	4
Reserved	1

- 5    MessageID                 The access terminal shall set this field to 0x00.
- 6    TransactionID            The access terminal shall increment this field every time it sends a  
 7                              new FixedModeRequest message.
- 8    DRCCover                The access terminal shall set this field to the DRC cover associated  
 9                              with the sector in its Active Set from which it wants to receive  
 10                          packets on the Forward Traffic Channel.
- 11   RequestedRate            The access terminal shall set this field to one of the valid DRC values  
 12                              in Table 8.4.5.5.1.1-1 to indicate the rate at which it wants to receive  
 13                          packets.
- 14   Reserved                The access terminal shall set this field to zero. The access network  
 15                          shall ignore this field.

<b>Channels</b>	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

## 17    8.4.6.3 FixedModeResponse

18   The access network sends the FixedModeResponse message to acknowledge the transition  
 19   to the Fixed Rate State.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
TransactionID	8

- 21   MessageID                The access network shall set this field to 0x01.

- 1 TransactionID The access network shall set this field to the TransactionID field of  
2 the associated FixedModeRequest message.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

#### 8.4.6.4 Configuration Messages

The Default Forward Traffic Channel MAC Protocol uses the Generic Configuration Protocol to exchange configuration parameters between the access network and the access terminal (see 10.7).

#### 8.4.6.4.1 Configurable Attributes

The following attributes and default values are defined:

#### 8.4.6.4.1.1 Simple Attributes

The negotiable simple attribute for this protocol is listed in Table 8.4.6.4-1. The access terminal shall use as defaults the values in Table 8.4.6.4-1 typed in ***bold italics***.

**Table 8.4.6.4-1. Configurable Values**

<b>Attribute ID</b>	<b>Attribute</b>	<b>Values</b>	<b>Meaning</b>
0xff	DRCGating	<b>0x0000</b>	Continuous transmission
		0x0001	Discontinuous transmission

The access terminal shall support the default value of this attribute.

#### 8.4.6.4.1.2 HandoffDelays Attribute

The following HandoffDelays complex attribute and default values are defined:

<b>Field</b>	<b>Length (bits)</b>	<b>Default</b>
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
SofterHandoffDelay	8	0x08
SoftHandoffDelay	8	0x10

- 1    Length                         Length of the complex attribute in octets. The access network shall  
 2                                     set this field to the length of the complex attribute excluding the  
 3                                     Length field.
- 4    AttributeID                 The access network shall set this field to 0x00.
- 5    ValueID                         The access network shall set this field to an identifier assigned to this  
 6                                     complex value.
- 7    SofterHandoffDelay             The access network shall set this field to the minimum interruption  
 8                                     seen by the access terminal when the access terminal switches the  
 9                                     DRC from a source sector to a target sector where the target sector is  
 10                                    such that its Forward Traffic Channel carries the same closed-loop  
 11                                    power control bits as the source sector (see SofterHandoff field of the  
 12                                    Route Update Protocol TrafficChannelAssignment message). The  
 13                                    access network shall specify this field in units of 8 slots. The access  
 14                                    terminal may use this number to adjust its algorithm controlling DRC  
 15                                    switching. The access terminal shall support all the values of this  
 16                                    attribute.
- 17    SoftHandoffDelay                 The access network shall set this field to the minimum interruption  
 18                                     seen by the access terminal when the access terminal switches the  
 19                                     DRC from a source sector to a target sector where the target sector is  
 20                                     such that its Forward Traffic Channel does not always carry the same  
 21                                     closed-loop power control bits as the source sector (see SoftHandoff  
 22                                     field of the Route Update Protocol TrafficChannelAssignment  
 23                                     message). The access network shall specify this field in units of 8  
 24                                     slots. The access terminal may use this number to adjust its  
 25                                     algorithm controlling DRC switching. The access terminal shall  
 26                                     support all the values of this attribute.
- 27    8.4.6.4.2 ConfigurationRequest  
 28                                     The ConfigurationRequest message format is given as part of the Generic Configuration  
 29                                     Protocol (see 10.7).
- 30                                     The MessageID field for this message shall be set to 0x50.

<b>Channels</b>	CC	FTC	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>			unicast	<b>Priority</b>	40

#### 8.4.6.4.3 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the access terminal includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response and shall set the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

<b>Channels</b>	CC	FTC	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>			unicast	<b>Priority</b>	40

<sup>1</sup> 8.4.7 Protocol Numeric Constants

Constant	Meaning	Value
N <sub>FTCMPType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>FTCMPDefault</sub>	Subtype field for this protocol	0x0000
N <sub>FTCMPPRestartTx</sub>	Number of consecutive slots of non-null rate DRCs to re-enable the Reverse Traffic Channel transmitter once it is disabled due to DRC supervision failure.	16
T <sub>FTCMPATFixedMode</sub>	Time the access terminal waits for the access network to acknowledge a transition to the Fixed Mode State.	1 second
T <sub>FTCMPANFixedMode</sub>	Time the access network has to acknowledge a transition to the Fixed Mode State	0.9 second
T <sub>FTCMDRCSupervision</sub>	DRC supervision timer	240 ms
T <sub>FTCMPPRestartTx</sub>	Reverse Channel Restart Timer	12 Control Channel cycles

<sup>2</sup> 8.4.8 Interface to Other Protocols

<sup>3</sup> 8.4.8.1 Commands Sent

<sup>4</sup> This protocol does not issue any commands.

<sup>5</sup> 8.4.8.2 Indications

<sup>6</sup> This protocol registers to receive the following indication:

- <sup>7</sup> • *PhysicalLayer.ForwardTrafficCompleted*

<sup>8</sup>

<sup>9</sup>

## 1   **8.5 Default Reverse Traffic Channel MAC Protocol**

### 2   8.5.1 Overview

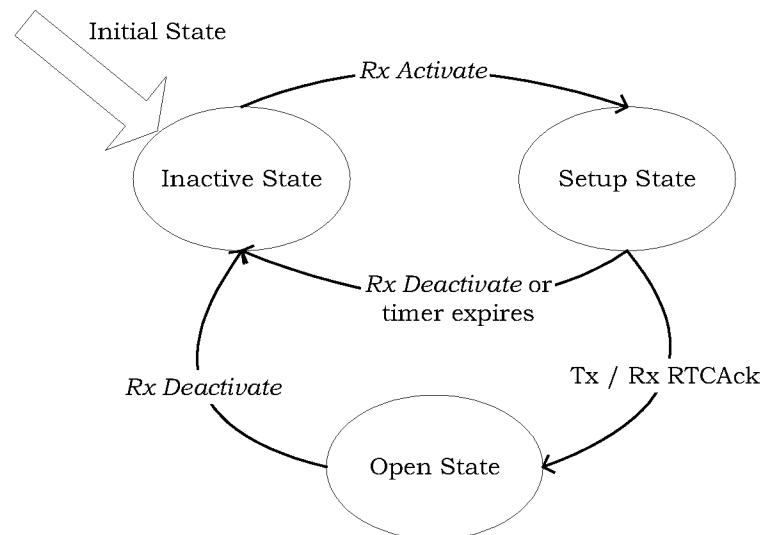
3   The Default Reverse Traffic Channel MAC Protocol provides the procedures and messages  
 4   required for an access terminal to transmit, and for an access network to receive the  
 5   Reverse Traffic Channel. Specifically, this protocol addresses Reverse Traffic Channel  
 6   transmission rules and rate control.

7   This specification assumes that the access network has one instance of this protocol for  
 8   every access terminal.

9   This protocol operates in one of three states:

- 10   • Inactive State: In this state, the access terminal is not assigned a Reverse Traffic  
 11   Channel. When the protocol is in this state, it waits for an *Activate* command.
- 12   • Setup State: In this state, the access terminal obeys the power control commands  
 13   that it receives from the access network. Data transmission on the Reverse Traffic  
 14   Channel is not allowed in this state.
- 15   • Open State: In this state, the access terminal may transmit data and negotiate  
 16   different transmission rates on the Reverse Traffic Channel.

17   The protocol states and the indications and events causing the transition between the  
 18   states are shown in Figure 8.5.1-1.



20   **Figure 8.5.1-1. Reverse Traffic Channel MAC Protocol State Diagram**

### 21   8.5.2 Primitives and Public Data

#### 22   8.5.2.1 Commands

23   This protocol defines the following commands:

- 1     • *Activate*
- 2     • *Deactivate*

3     8.5.2.2 Return Indications

4     This protocol returns the following indications:

- 5     • *LinkAcquired*

6     8.5.2.3 Public Data

7     This protocol shall make the following data public:

- 8       • RABLength for every pilot in the Active Set
- 9       • RABOffset for every pilot in the Active Set
- 10      • DataOffsetNom
- 11      • DataOffset9k6
- 12      • DataOffset19k2
- 13      • DataOffset38k4
- 14      • DataOffset76k8
- 15      • DataOffset153k6
- 16      • RPCStep
- 17      • MI<sub>RTCMAC</sub>
- 18      • MQ<sub>RTCMAC</sub>

19    8.5.3 Basic Protocol Numbers

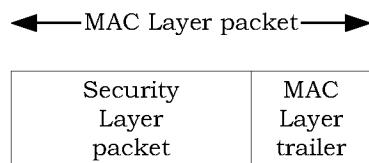
20    The Type field for this protocol is one octet, set to N<sub>RTCMPType</sub>.

21    The Subtype field for this protocol is two octets, set to N<sub>RTCMPDefault</sub>.

22    8.5.4 Protocol Data Unit

23    The transmission unit of this protocol is a Reverse Traffic Channel MAC Layer packet. Each  
24    packet contains one Security Layer packet.

25    The protocol constructs a packet out of the Security Layer packets by adding the MAC Layer  
26    trailer defined in 8.5.6.1. The protocol then sends the packet for transmission to the  
27    Physical Layer. The packet structure is shown in Figure 8.5.4-1



28  
29   **Figure 8.5.4-1. Reverse Traffic Channel MAC Layer Packet Structure**

- 1 If the MACLayerFormat field of the MAC Layer trailer is equal to '1', received packets are  
 2 passed for further processing to the Security Layer after removing the layer-related trailer.  
 3 The access network shall discard the MAC packet if the MACLayerFormat field of the MAC  
 4 Layer trailer is equal to '0'. The ConnectionLayerFormat field in the MAC Layer trailer shall  
 5 be passed to the Security Layer with the Security Layer packet.
- 6 The maximum size payload this protocol can support (i.e., the maximum size Security Layer  
 7 packet that can be carried) is a function of the transmission rate used on the Reverse  
 8 Traffic Channel. Table 8.5.4-1 provides the transmission rates and corresponding minimum  
 9 and maximum payload sizes available on the Reverse Traffic Channel.

10 **Table 8.5.4-1. Reverse Traffic Channel Rates and Payload**

<b>Transmission Rate (kbps)</b>	<b>Minimum Payload (bits)</b>	<b>Maximum Payload (bits)</b>
0.0	0	0
9.6	1	232
19.2	233	488
38.4	489	1000
76.8	1001	2024
153.6	2025	4072

## 11 8.5.5 Procedures

## 12 8.5.5.1 Protocol Initialization and Configuration

13 This protocol shall be started in the Inactive State.

14 Configuration parameters are provided by using the  
 15 ConfigurationRequest/ConfigurationResponse messages or by using a protocol constant.  
 16 Section 8.5.6.5.1 defines the attributes that can be configured and the default values that  
 17 the access terminal shall use unless superseded by a configuration exchange. Section 8.5.7  
 18 lists the protocol constants.

## 19 8.5.5.2 Command Processing

## 20 8.5.5.2.1 Activate

21 If the protocol receives an *Activate* command in the Inactive State, the access terminal and  
 22 the access network shall perform the following:

- 23 • Set ATI<sub>LCM</sub> to TransmitATI.ATI
- 24 • Transition to the Setup State

25 If the protocol receives this command in any other state it shall be ignored.

#### 8.5.5.2.2 Deactivate

2 If the protocol receives a *Deactivate* command in the Setup State or the Open State,

3     • Access terminal shall cease transmitting the Reverse Traffic Channel and shall  
4         transition to the Inactive State.

5     • Access network shall cease monitoring the Reverse Traffic Channel from this access  
6         terminal and shall transition to the Inactive State.

7 If the protocol receives a *Deactivate* command in the Inactive State, it shall be ignored.

#### 8.5.5.3 Reverse Traffic Channel Long Code Mask

9 The access terminal shall set the long code masks for the reverse traffic channel ( $MI_{RTCMAC}$   
10 and  $MO_{RTCMAC}$ ) as shown in Table 8.5.5.3-1.

**Table 8.5.5.3-1. Reverse Traffic Channel Long Code Masks**

Permuted (ATI<sub>LCM</sub>) is defined as follows:

$$\text{ATI}_{\text{LCM}} = (\text{A}_{31}, \text{A}_{30}, \text{A}_{29}, \dots, \text{A}_0)$$

Permuted (ATI<sub>LCM</sub>) =

$(A_0, A_{31}, A_{22}, A_{13}, A_4, A_{26}, A_{17}, A_8, A_{30}, A_{21}, A_{12}, A_3, A_{25}, A_{16}, A_7, A_{29}, A_{20}, A_{11}, A_2, A_{24}, A_{15}, A_6, A_{28}, A_{19}, A_{10}, A_1, A_{23}, A_{14}, A_5, A_{27}, A_{18}, A_9)$ .

Permuted (ATI<sub>LCM</sub>)' is bitwise complement of Permuted (ATI<sub>LCM</sub>).

#### 8.5.5.4 Inactive State

When the protocol is in the Inactive State the access terminal and the access network wait for an *Activate* command.

#### 8.5.5.5 Setup State

#### 8.5.5.5.1 Access Terminal Requirements

24 The access terminal shall set a timer for  $T_{\text{RTCPATSetup}}$  seconds when it enters this state. If  
25 the protocol is still in the Setup State when the timer expires, the access terminal shall  
26 cease transmission on the Reverse Traffic Channel and transition to the Inactive State.

27 The access terminal shall start transmission on the reverse Traffic Channel upon entering  
28 this state, and shall obey the Reverse Power Control Channel. The access terminal shall set  
29 the DRC value and cover as specified in the Forward Traffic Channel MAC Protocol.

30 The access terminal shall not transmit any data on the Reverse Traffic Data Channel while  
31 in this state.

1 If the access terminal receives an RTCAck message it shall return a *LinkAcquired* indication  
 2 and transition to the Open State.

3 8.5.5.5.2 Access Network Requirements

4 The access network shall set a timer for  $T_{RTCPANSetup}$  seconds when it enters this state. If  
 5 the protocol is still in the Setup State when the timer expires, the access network shall  
 6 transition to the Inactive State.

7 The access network shall attempt to acquire the Reverse Traffic Channel in this state. If the  
 8 access network acquires the Reverse Traffic Channel, it shall send an RTCAck message to  
 9 the access terminal, return a *LinkAcquired* indication, and shall transition to the Open  
 10 State.

11 8.5.5.6 Open State

12 8.5.5.6.1 Frame Offset Delay

13 The access terminal shall delay the Reverse Traffic Data Channel and Reverse Rate  
 14 Indicator Channel (RRI) transmissions by FrameOffset slots with respect to the system-  
 15 time-aligned frame boundary.

16 8.5.5.6.2 Rate Control

17 The description in this section uses the following variables: MaxRate, CurrentRate,  
 18 CombinedBusyBit, and CurrentRateLimit.

19 CurrentRateLimit shall be set initially to 9.6kbps. After a BroadcastReverseRateLimit  
 20 message or a UnicastReverseRateLimit message is received by the access terminal, the  
 21 access terminal shall update the CurrentRateLimit value as follows:

- 22 • If the RateLimit value in the message is less than or equal to the CurrentRateLimit  
 23 value, the access terminal shall set CurrentRateLimit to the RateLimit value in the  
 24 message immediately after the receipt of the message.
- 25 • If the RateLimit value in the message is greater than the CurrentRateLimit value,  
 26 then the access terminal shall set CurrentRateLimit to the RateLimit value in the  
 27 message, one frame (16 slots) after the message is received.

28 If the last received reverse activity bit is set to '1' from any sector in the access terminal's  
 29 active set, the access terminal shall set CombinedBusyBit to '1'. Otherwise, the access  
 30 terminal shall set CombinedBusyBit to '0'.

31 CurrentRate shall be set to the rate at which the access terminal was transmitting data  
 32 immediately before the new transmission time. If the access terminal was not transmitting  
 33 data immediately before the new transmission time, the access terminal shall set  
 34 CurrentRate to 0.

35 The access terminal sets the variable MaxRate based on its current transmission rate, the  
 36 value of the CombinedBusyBit, and a random number. The access terminal shall generate a  
 37 random number  $x$ , uniformly distributed between 0 and 1. The access terminal shall  
 38 evaluate the condition shown in Table 8.5.5.6.2-1 based on the values of CurrentRate,

- 1 CombinedBusyBit, and Condition. If the Condition is true, the access terminal shall set  
 2 MaxRate to the MaxRateTrue value for the corresponding row in Table 8.5.5.6.2-1.  
 3 Otherwise, the access terminal shall set MaxRate to the MaxRateFalse value for the  
 4 corresponding row in Table 8.5.5.6.2-1.

5 **Table 8.5.5.6.2-1. Determination of MaxRate**

<b>CurrentRate</b>	<b>Combined BusyBit</b>	<b>Condition</b>	<b>MaxRateTrue</b>	<b>MaxRateFalse</b>
0	'0'	True	9.6kbps	N/A
9.6kbps	'0'	$x < \text{Transition009k6\_019k2}$	19.2kbps	9.6kbps
19.2kbps	'0'	$x < \text{Transition019k2\_038k4}$	38.4kbps	19.2kbps
38.4kbps	'0'	$x < \text{Transition038k4\_076k8}$	76.8kbps	38.4kbps
76.8kbps	'0'	$x < \text{Transition076k8\_153k6}$	153.6kbps	76.8kbps
153.6kbps	'0'	False	N/A	153.6kbps
0	'1'	False	N/A	9.6kbps
9.6kbps	'1'	False	N/A	9.6kbps
19.2kbps	'1'	$x < \text{Transition019k2\_009k6}$	9.6kbps	19.2kbps
38.4kbps	'1'	$x < \text{Transition038k4\_019k2}$	19.2kbps	38.4kbps
76.8kbps	'1'	$x < \text{Transition076k8\_038k4}$	38.4kbps	76.8kbps
153.6kbps	'1'	$x < \text{Transition153k2\_076k8}$	76.8kbps	153.6kbps

- 6
- 7 The access terminal shall select a transmission rate that satisfies the following constraints:
- 8     • The access terminal shall transmit at a rate that is no greater than the value of  
 9       MaxRate.
- 10     • The access terminal shall transmit at a rate that is no greater than the value of  
 11       CurrentRateLimit.
- 12     • The access terminal shall transmit at a data rate no higher than the highest data  
 13       rate that can be accommodated by the available transmit power.
- 14     • The access terminal shall not select a data rate for which the minimum payload  
 15       length, as specified in Table 8.5.4-1, is greater than the size of data it has to send.

16     8.5.5.6.3 Power Control

17     The access terminal shall control the reverse link transmit power in accordance with the  
 18       requirements of the Physical Layer Protocol.

19     8.5.6 Trailer and Message Formats

20       8.5.6.1 MAC Layer Trailer

21     The access terminal shall set the MAC Layer trailer as follows:

<b>Field</b>	<b>Length (bits)</b>
ConnectionLayerFormat	1
MACLayerFormat	1

## 2 ConnectionLayerFormat

3 The access terminal shall set this field to '1' if the connection layer  
 4 packet is Format B; otherwise, the access terminal shall set this field  
 5 to '0'.

## 6 MACLayerFormat

7 The access terminal shall set this field to '1' if the MAC layer packet  
 8 contains a valid payload; otherwise, the access terminal shall set this  
 field to '0'.

## 9 8.5.6.2 RTCAck

10 The access network sends the RTCAck message to notify the access terminal that it has  
 11 acquired the Reverse Traffic Channel. The access network shall send this message using  
 12 the access terminal's current ATI.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8

## 14 MessageID

15 The access network shall set this field to 0x00.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Best Effort
<b>Addressing</b>		unicast	<b>Priority</b>	10

## 16 8.5.6.3 BroadcastReverseRateLimit

17 The BroadcastReverseRateLimit message is used by the access network to control the  
 18 transmission rate on the reverse link.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
RPCCount	6

17 RPCCount occurrences of the following field

RateLimit	4
Reserved	Variable

## 20 MessageID

The access network shall set this field to 0x01.

- 1    RPCCount                         The access network shall set this value to the maximum number of  
2                                         RPC channels supported by the sector.
- 3    RateLimit                         The access network shall set occurrence  $n$  of this field to the highest  
4                                         data rate that the access terminal associated with MACIndex  $64-n$  is  
5                                         allowed to use on the Reverse Traffic Channel, as shown in Table  
6                                         8.5.6.3-1.

7                                         **Table 8.5.6.3-1. Encoding of the RateLimit Field**

<b>Field value</b>	<b>Meaning</b>
0x0	0 kbps
0x1	9.6 kbps
0x2	19.2 kbps
0x3	38.4 kbps
0x4	76.8 kbps
0x5	153.6 kbps
All other values	Invalid

- 8    Reserved                         The number of bits in this field is equal to the number needed to  
9                                         make the message length an integer number of octets. The access  
10                                        network shall set this field to zero. The access terminal shall ignore  
11                                        this field.

<b>Channels</b>	CC	<b>SLP</b>	Best Effort
<b>Addressing</b>	broadcast	<b>Priority</b>	40

13                                         **8.5.6.4 UnicastReverseRateLimit**

- 14                                         The UnicastReverseRateLimit message is used by the access network to control the  
15                                         transmission rate on the reverse link for a particular access terminal.

<b>Field</b>	<b>Length (bits)</b>
MessageID	8
RateLimit	4
Reserved	4

- 17    MessageID                         The access network shall set this field to 0x02.
- 18    RateLimit                         The access network shall set this field to the highest data rate that  
19                                         the access terminal is allowed to use on the Reverse Traffic Channel,  
20                                         as shown in Table 8.5.6.4-1.

**Table 8.5.6.4-1. Encoding of the RateLimit Field**

<b>Field value</b>	<b>Meaning</b>
0x0	0 kbps
0x1	9.6 kbps
0x2	19.2 kbps
0x3	38.4 kbps
0x4	76.8 kbps
0x5	153.6 kbps
All other values	Invalid

Reserved The number of bits in this field is equal to the number needed to make the message length an integer number of octets. The access network shall set this field to zero. The access terminal shall ignore this field.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

### 8.5.6.5 Configuration Messages

The Default Reverse Traffic Channel MAC Protocol uses the Generic Configuration Protocol to transmit configuration parameters from the access network to the access terminal.

### 10 8.5.6.5.1 Configurable Attributes

11 The following configurable attributes are defined:

1    8.5.6.5.1.1 PowerParameters Attribute  
2

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
DataOffsetNom	4	0
DataOffset9k6	4	0
DataOffset19k2	4	0
DataOffset38k4	4	0
DataOffset76k8	4	0
DataOffset153k6	4	0
RPCStep	2	1
Reserved	2	N/A

- 3    Length                         Length of the complex attribute in octets. The access network shall  
4                                        set this field to the length of the complex attribute excluding the  
5                                        Length field.
- 6    AttributeID                  The access network shall set this field to 0x00.
- 7    ValueID                        The access network shall set this field to an identifier assigned to this  
8                                        complex value.
- 9    DataOffsetNom                The access network shall set this field to the nominal offset of the  
10                                      reverse link data channel power to pilot channel power, expressed as  
11                                      2's complement value in units of 0.5 dB. The access terminal shall  
12                                      support all the valid values specified by this field.
- 13   DataOffset9k6                The access network shall set this field to the ratio of reverse link data  
14                                      channel power at 9.6 kbps to the nominal reverse link data channel  
15                                      power at 9.6 kbps, expressed as 2's complement in units of 0.25 dB.  
16                                      The access terminal shall support all the valid values specified by this  
17                                      field.
- 18   DataOffset19k2                The access network shall set this field to the ratio of reverse link data  
19                                      channel power at 19.2 kbps to the nominal reverse link data channel  
20                                      power at 19.2 kbps, expressed as 2's complement in units of 0.25 dB.  
21                                      The access terminal shall support all the valid values specified by this  
22                                      field.

- 1 DataOffset38k4 The access network shall set this field to the ratio of reverse link data  
 2 channel power at 38.4 kbps to the nominal reverse link data channel  
 3 power at 38.4 kbps, expressed as 2's complement in units of 0.25 dB.  
 4 The access terminal shall support all the valid values specified by this  
 5 field.
- 6 DataOffset76k8 The access network shall set this field to the ratio of reverse link data  
 7 channel power at 76.8 kbps to the nominal reverse link data channel  
 8 power at 76.8 kbps, expressed as 2's complement in units of 0.25 dB.  
 9 The access terminal shall support all the valid values specified by this  
 10 field.
- 11 DataOffset153k6 The access network shall set this field to the ratio of reverse link data  
 12 channel power at 153.6 kbps to the nominal reverse link data channel  
 13 power at 153.6 kbps, expressed as 2's complement in units  
 14 of 0.25 dB. The access terminal shall support all the valid values  
 15 specified by this field.
- 16 RPCStep Reverse Power Control step. The access network shall set this field to  
 17 the power control step size the access terminal shall use when  
 18 controlling the power of the reverse link, as shown in Table  
 19 8.5.6.5.1.1-1. The access terminal shall support all the valid values  
 20 specified by this field.

21 **Table 8.5.6.5.1.1-1. Encoding of the RPCStep Field**

<b>Field value (binary)</b>	<b>Meaning</b>
'00'	0.5 dB
'01'	1.0 dB
All other values	Invalid

- 22 Reserved The access network shall set this field to zero. The access terminal  
 23 shall ignore this field.  
 24

## 1    8.5.6.5.1.2 RateParameters Attribute

2

Field	Length (bits)	Default
Length	8	N/A
AttributeID	8	N/A

One or more of the following record:

ValueID	8	N/A
Transition009k6_019k2	4	0xB
Transition019k2_038k4	4	0x4
Transition038k4_076k8	4	0x2
Transition076k8_153k6	4	0x2
Transition019k2_009k6	4	0x4
Transition038k4_019k2	4	0x4
Transition076k8_038k4	4	0x8
Transition153k6_076k8	4	0xF

- 3    Length                 Length of the complex attribute in octets. The access network shall  
4                            set this field to the length of the complex attribute excluding the  
5                            Length field.
- 6    AttributeID          The access network shall set this field to 0x01.
- 7    ValueID                The access network shall set this field to an identifier assigned to this  
8                            complex value.
- 9    Transition009k6\_019k2         The field is set to indicate the probability the access terminal shall  
10                            use to increase its transmission rate if its current transmission rate  
11                            is 9.6 kbps. See Table 8.5.6.5.1.2-1 for the probability associated with  
12                            each value of the field. The access terminal shall support all the valid  
13                            values specified by this field.
- 14
- 15    Transition019k2\_038k4         The field is set to indicate the probability the access terminal shall  
16                            use to increase its transmission rate if its current transmission rate  
17                            is 19.2 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
18                            with each value of the field. The access terminal shall support all the  
19                            valid values specified by this field.
- 20
- 21    Transition038k4\_076k8         The field is set to indicate the probability the access terminal shall  
22                            use to increase its transmission rate if its current transmission rate  
23

1           is 38.4 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
2           with each value of the field. The access terminal shall support all the  
3           valid values specified by this field.

4           Transition076k8\_153k6

5           The field is set to indicate the probability the access terminal shall  
6           use to increase its transmission rate if its current transmission rate  
7           is 76.8 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
8           with each value of the field. The access terminal shall support all the  
9           valid values specified by this field.

10          Transition019k2\_009k6

11          The field is set to indicate the probability the access terminal shall  
12          use to decrease its transmission rate if its current transmission rate  
13          is 19.2 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
14          with each value of the field. The access terminal shall support all the  
15          valid values specified by this field.

16          Transition038k4\_019k2

17          The field is set to indicate the probability the access terminal shall  
18          use to decrease its transmission rate if its current transmission rate  
19          is 38.4 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
20          with each value of the field. The access terminal shall support all the  
21          valid values specified by this field.

22          Transition076k8\_038k4

23          The field is set to indicate the probability the access terminal shall  
24          use to decrease its transmission rate if its current transmission rate  
25          is 76.8 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
26          with each value of the field. The access terminal shall support all the  
27          valid values specified by this field.

28          Transition153k6\_076k8

29          The field is set to indicate the probability the access terminal shall  
30          use to decrease its transmission rate if its current transmission rate  
31          is 153.6 kbps. See Table 8.5.6.5.1.2-1 for the probability associated  
32          with each value of the field. The access terminal shall support all the  
33          valid values specified by this field.

**Table 8.5.6.5.1.2-1. Probability Table for the RateParameters Attribute**

<b>Value</b>	<b>Probability</b>
0x0	0.0000
0x1	0.0625
0x2	0.1250
0x3	0.1875
0x4	0.2500
0x5	0.3125
0x6	0.3750
0x7	0.4375
0x8	0.5000
0x9	0.6250
0xA	0.6875
0xB	0.7500
0xC	0.8125
0xD	0.8750
0xE	0.9375
0xF	1.0000

### 8.5.6.5.2 ConfigurationRequest

The ConfigurationRequest message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x50.

<b>Channels</b>	CC	FTC	<b>SLP</b>	Reliable
<b>Addressing</b>		unicast	<b>Priority</b>	40

### 8.5.6.5.3 ConfigurationResponse

The ConfigurationResponse message format is given as part of the Generic Configuration Protocol (see 10.7).

The MessageID field for this message shall be set to 0x51.

If the access terminal includes an attribute with this message, it shall set the AttributeID field of the message to the AttributeID field of the ConfigurationRequest message associated with this response, and shall set the ValueID field to the ValueID field of one of the complex attribute values offered by the ConfigurationRequest message.

<b>Channels</b>	RTC	<b>SLP</b>	Reliable
<b>Addressing</b>	unicast	<b>Priority</b>	40

1 8.5.7 Protocol Numeric Constants

<b>Constant</b>	<b>Meaning</b>	<b>Value</b>
N <sub>RTCMType</sub>	Type field for this protocol	Table 2.3.6-1
N <sub>RTCMPDefault</sub>	Subtype field for this protocol	0x0000
T <sub>RTCPATSetup</sub>	Maximum time for the access terminal to transmit the Reverse Traffic Channel in the Setup State	1.5 seconds
T <sub>RTCPANSetup</sub>	Maximum time for the access network to acquire the Reverse Traffic Channel and send a notification to the access terminal.	1 second

2 8.5.8 Interface to Other Protocols

3 8.5.8.1 Commands Sent

4 This protocol does not issue any commands.

5 8.5.8.2 Indications

6 This protocol does not register to receive any indications.

7

1 No text.



## 1 **9 PHYSICAL LAYER**

### 2 **9.1 Physical Layer Packets**

#### 3 **9.1.1 Overview**

4 The transmission unit of the physical layer is a physical layer packet. A physical layer  
 5 packet can be of length 256, 512, 1024, 2048, 3072, or 4096 bits. The format of the  
 6 physical layer packet depends upon which channel it is transmitted on. A physical layer  
 7 packet carries one or more MAC layer packets.

#### 8 **9.1.2 Physical Layer Packet Formats**

##### 9 **9.1.2.1 Control Channel Physical Layer Packet Format**

10 The length of a Control Channel physical layer packet shall be 1024 bits. Each Control  
 11 Channel physical layer packet shall carry one Control Channel MAC layer packet. Control  
 12 Channel physical layer packets shall use the following format:

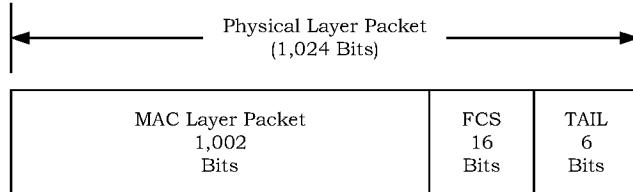
<b>Field</b>	<b>Length (bits)</b>
MAC Layer Packet	1,002
FCS	16
TAIL	6

14           MAC Layer Packet - MAC layer packet from the Control Channel MAC protocol.

15           FCS - Frame check sequence (see 9.1.4).

16           TAIL - Encoder tail bits. This field shall be set to all '0's.

17         Figure 9.1.2.1-1 illustrates the format of the Control Channel physical layer packets.



19 **Figure 9.1.2.1-1. Physical Layer Packet Format for the Control Channel**

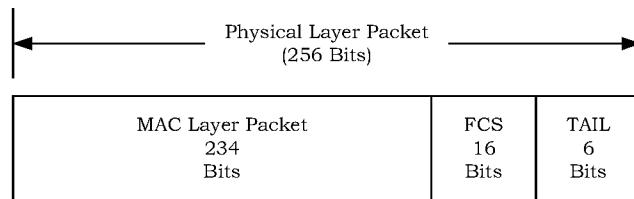
#### 21 **9.1.2.2 Access Channel Physical Layer Packet Format**

22 The length of an Access Channel physical layer packet shall be 256 bits. Each Access  
 23 Channel physical layer packet shall carry one Access Channel MAC layer packet. Access  
 24 Channel physical layer packets shall use the following format:

Field	Length (bits)
MAC Layer Packet	234
FCS	16
TAIL	6

- 1
- 2 MAC Layer Packet - MAC layer packet from the Access Channel MAC protocol.
- 3 FCS - Frame check sequence (see 9.1.4).
- 4 TAIL - Encoder tail bits. This field shall be set to all '0's.

5 Figure 9.1.2.2-1 illustrates the format of the Access Channel physical layer packets.



7 **Figure 9.1.2.2-1. Physical Layer Packet Format for the Access Channel**

8 9.1.2.3 Forward Traffic Channel Physical Layer Packet Format

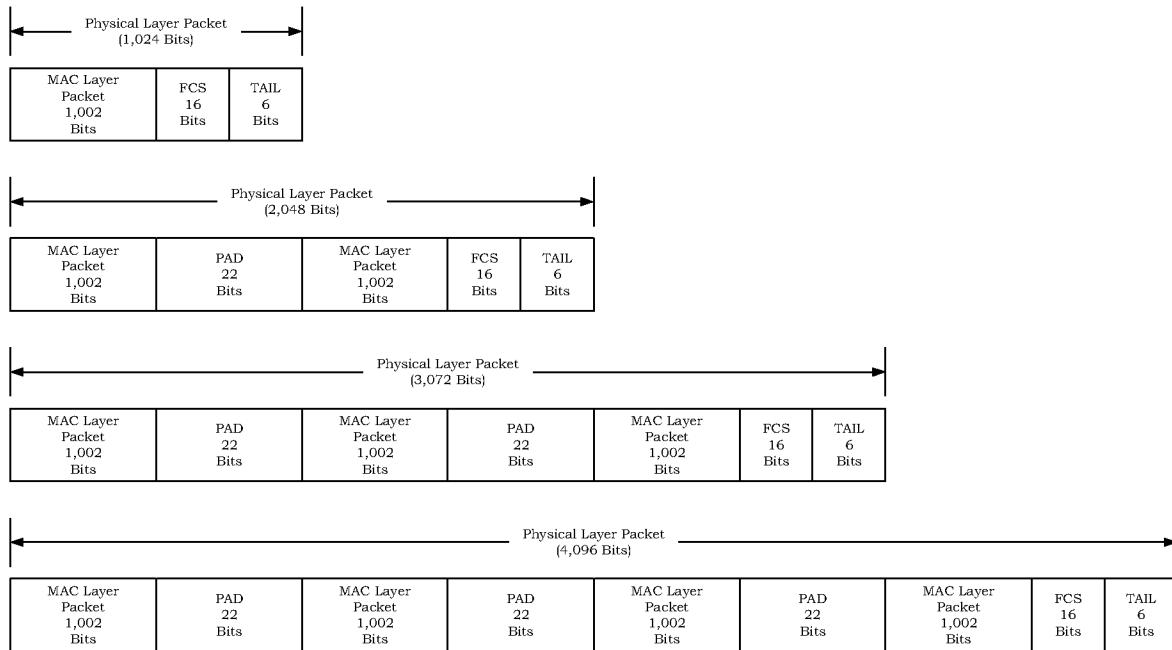
9 The length of a Forward Traffic Channel physical layer packet shall be 1024, 2048, 3072, or  
 10 4096 bits. A Forward Traffic Channel physical layer packet shall carry 1, 2, 3, or 4 Forward  
 11 Traffic Channel MAC layer packets depending on the rate of transmission. Forward Traffic  
 12 Channel physical layer packets shall use the following format:

Field	Length (bits)
0, 1, 2, or 3 occurrences of the following two fields:	
MAC Layer Packet	1,002
PAD	22
One occurrence of the following three fields:	
MAC Layer Packet	1,002
FCS	16
TAIL	6

- 14
- 15 MAC Layer Packet - MAC layer packet from the Forward Traffic Channel MAC Protocol.
- 16 PAD - This field shall be set to all '0's. The receiver shall ignore this field.
- 17 FCS - Frame check sequence (see 9.1.4).

1           TAIL - Encoder tail bits. This field shall be set to all '0's.

2       Figure 9.1.2.3-1 illustrates the format of the Forward Traffic Channel physical layer  
3       packets.



5       **Figure 9.1.2.3-1. Physical Layer Packet Format for the Forward Traffic Channel**

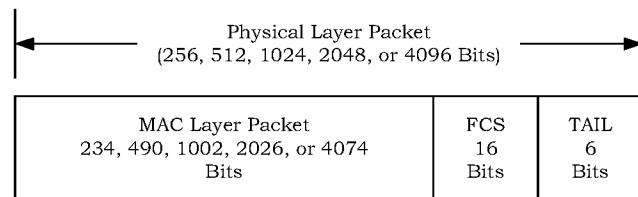
#### 6       9.1.2.4 Reverse Traffic Channel Physical Layer Packet Format

7       The length of a Reverse Traffic Channel physical layer packet shall be 256, 512, 1024,  
8       2048, or 4096 bits. Each Reverse Traffic Channel physical layer packet shall carry one  
9       Reverse Traffic Channel MAC layer packet. Reverse Traffic Channel physical layer packets  
10      shall use the following format:

Field	Length (bits)
MAC Layer Packet	234, 490, 1002, 2026, or 4074
FCS	16
TAIL	6

- 12
- 13       MAC Layer Packet - MAC layer packet from the Reverse Traffic Channel MAC  
14       Protocol.
  - 15       FCS - Frame check sequence (see 9.1.4).
  - 16       TAIL - Encoder tail bits. This field shall be set to all '0's.

17       Figure 9.1.2.4-1 illustrates the format of the Reverse Traffic Channel physical layer packets.



**Figure 9.1.2.4-1. Physical Layer Packet Format for the Reverse Traffic Channel**

### 9.1.3 Bit Transmission Order

Each field of the physical layer packets shall be transmitted in sequence such that the most significant bit (MSB) is transmitted first and the least significant bit (LSB) is transmitted last. The MSB is the left-most bit in the figures of the document.

### 9.1.4 Computation of the FCS Bits

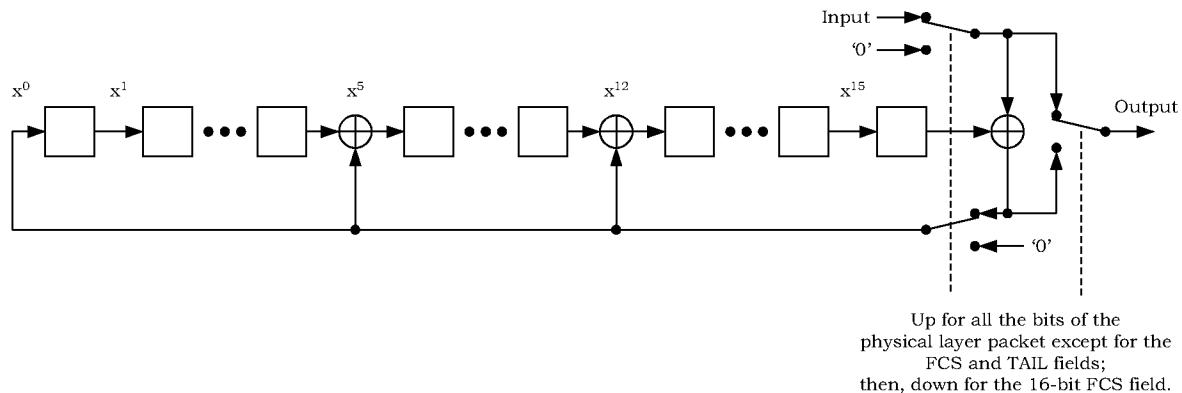
The FCS computation described here shall be used for computing the FCS field in the Control Channel physical layer packets, the Forward Traffic Channel physical layer packets, the Access Channel physical layer packets, and the Reverse Traffic Channel physical layer packets.

The FCS shall be a CRC calculated using the standard CRC-CCITT generator polynomial:

$$g(x) = x^{16} + x^{12} + x^5 + 1.$$

The FCS shall be equal to the value computed according to the following procedure as shown in Figure 9.1.4-1:

- All shift-register elements shall be initialized to '0's.
- The switches shall be set in the up position.
- The register shall be clocked once for each bit of the physical layer packet except for the FCS and TAIL fields. The physical layer packet shall be read from MSB to LSB.
- The switches shall be set in the down position so that the output is a modulo-2 addition with a '0' and the successive shift-register inputs are '0's.
- The register shall be clocked an additional 16 times for the 16 FCS bits.
- The output bits constitute all fields of the physical layer packets except the TAIL field.



**Figure 9.1.4-1. FCS Computation for the Physical Layer Packet**

1

2

3

1    **9.2 Access Terminal Requirements**

2    This section defines requirements specific to access terminal equipment and operation.

3    9.2.1 Transmitter

4    9.2.1.1 Frequency Parameters

5    9.2.1.1.1 Channel Spacing and Designation

6    9.2.1.1.1.1 Band Class 0 (800-MHz Band)

7    The Band Class 0 system designators for the access terminal and access network shall be  
8    as specified in Table 9.2.1.1.1-1.

9    There are two band subclasses specified for Band Class 0. Access terminals supporting  
10   Band Class 0 shall support at least one band subclass belonging to Band Class 0.

11   Access terminals supporting Band Class 0 shall be capable of transmitting in Band Class 0.

12   The channel spacing, CDMA channel designations, and transmitter center frequencies of  
13   Band Class 0 shall be as specified in Table 9.2.1.1.1-2. Access terminals supporting Band  
14   Class 0 shall support transmission on the valid channel numbers shown in Table  
15   9.2.1.1.1-3.<sup>41</sup>

16   The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the  
17   frequency of the access network transmit signal as measured at the access terminal  
18   receiver.

19   **Table 9.2.1.1.1-1. Band Class 0 System Frequency Correspondence**

<b>System Designator</b>	<b>Band Subclass</b>	<b>Transmit Frequency Band (MHz)</b>	
		<b>Access Terminal</b>	<b>Access Network</b>
A	0	824.025–835.005 844.995–846.495	869.025–880.005 889.995–891.495
	1	824.025–835.005 844.995–848.985	869.025–880.005 889.995–893.985
B	0	835.005–844.995 846.495–848.985	880.005–889.995 891.495–893.985
	1	835.005–844.995	880.005–889.995

20

---

<sup>41</sup> Note that the Korean Cellular Band uses Band Subclass 1 and has additional valid channels that a Band Class 0 access terminal should support to permit roaming to Korea.

1                   **Table 9.2.1.1.1.1-2. CDMA Channel Number to CDMA Frequency Assignment**  
2                   Correspondence for Band Class 0

<b>Transmitter</b>	<b>CDMA Channel Number</b>	<b>Center Frequency for CDMA Channel (MHz)</b>
Access Terminal	$1 \leq N \leq 799$	$0.030 N + 825.000$
	$991 \leq N \leq 1023$	$0.030 (N - 1023) + 825.000$
Access Network	$1 \leq N \leq 799$	$0.030 N + 870.000$
	$991 \leq N \leq 1023$	$0.030 (N - 1023) + 870.000$

3

1      **Table 9.2.1.1.1.1-3. CDMA Channel Numbers and Corresponding Frequencies for Band**  
 2      **Class 0**

<b>Band Subclass</b>	<b>System Designator</b>	<b>CDMA Channel Validity</b>	<b>CDMA Channel Number</b>	<b>Transmit Frequency Band (MHz)</b>	
				<b>Access Terminal</b>	<b>Access Network</b>
0	A'' (1 MHz)	Not Valid	991–1012	824.040–824.670	869.040–869.670
		Valid	1013–1023	824.700–825.000	869.700–870.000
	A (10 MHz)	Valid	1–311	825.030–834.330	870.030–879.330
		Not Valid	312–333	834.360–834.990	879.360–879.990
	B (10 MHz)	Not Valid	334–355	835.020–835.650	880.020–880.650
		Valid	356–644	835.680–844.320	880.680–889.320
		Not Valid	645–666	844.350–844.980	889.350–889.980
	A' (1.5 MHz)	Not Valid	667–688	845.010–845.640	890.010–890.640
		Valid	689–694	845.670–845.820	890.670–890.820
		Not Valid	695–716	845.850–846.480	890.850–891.480
	B' (2.5 MHz)	Not Valid	717–738	846.510–847.140	891.510–892.140
		Valid	739–777	847.170–848.310	892.170–893.310
		Not Valid	778–799	848.340–848.970	893.340–893.970
1	A'' (1 MHz)	Not Valid	991–1012	824.040–824.670	869.040–869.670
		Valid	1013–1023	824.700–825.000	869.700–870.000
	A (10 MHz)	Valid	1–311	825.030–834.330	870.030–879.330
		Not Valid	312–333	834.360–834.990	879.360–879.990
	B (10 MHz)	Not Valid	334–355	835.020–835.650	880.020–880.650
		Valid	356–644	835.680–844.320	880.680–889.320
		Not Valid	645–666	844.350–844.980	889.350–889.980
	A' (1.5 MHz)	Not Valid	667–688	845.010–845.640	890.010–890.640
		Valid	689–716	845.670–846.480	890.670–891.480
	A''' (2.5 MHz)	Valid	717–779	846.510–848.370	891.510–893.370
		Not Valid	780–799	848.400–848.970	893.400–893.970

3

4      **9.2.1.1.1.2 Band Class 1 (1900-MHz Band)**

5      The Band Class 1 block designators for the access terminal and access network shall be as  
 6      specified in Table 9.2.1.1.1.2-1.

7      Access terminals supporting Band Class 1 shall be capable of transmitting in Band Class 1.

8      The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 9      Band Class 1 shall be as specified in Table 9.2.1.1.1.2-2. Access terminals supporting Band  
 10     Class 1 shall support transmission on the valid and conditionally valid channel numbers  
 11     shown in Table 9.2.1.1.1.2-3. Note that certain channel assignments are not valid and  
 12     others are conditionally valid. Transmission on conditionally valid channels is permissible if

1 the adjacent block is allocated to the same licensee or if other valid authorization has been  
 2 obtained.

3 The nominal access terminal transmit carrier frequency shall be 80.0 MHz lower than the  
 4 frequency of the access network transmit signal as measured at the access terminal  
 5 receiver.

6 **Table 9.2.1.1.2-1. Band Class 1 Block Frequency Correspondence**

<b>Block Designator</b>	<b>Transmit Frequency Band (MHz)</b>	
	<b>Access Terminal</b>	<b>Access Network</b>
A	1850–1865	1930–1945
D	1865–1870	1945–1950
B	1870–1885	1950–1965
E	1885–1890	1965–1970
F	1890–1895	1970–1975
C	1895–1910	1975–1990

7

8 **Table 9.2.1.1.2-2. CDMA Channel Number to CDMA Frequency Assignment  
 9 Correspondence for Band Class 1**

<b>Transmitter</b>	<b>CDMA Channel Number</b>	<b>Center Frequency for CDMA Channel (MHz)</b>
Access Terminal	$0 \leq N \leq 1199$	$1850.000 + 0.050 N$
Access Network	$0 \leq N \leq 1199$	$1930.000 + 0.050 N$

10

1           **Table 9.2.1.1.1.2-3. CDMA Channel Numbers and Corresponding Frequencies**  
 2           **for Band Class 1**

<b>Block Designator</b>	<b>CDMA Channel Validity</b>	<b>CDMA Channel Number</b>	<b>Transmit Frequency Band (MHz)</b>	
			<b>Access Terminal</b>	<b>Access Network</b>
A (15 MHz)	Not Valid	0–24	1850.000–1851.200	1930.000–1931.200
	Valid	25–275	1851.250–1863.750	1931.250–1943.750
	Cond. Valid	276–299	1863.800–1864.950	1943.800–1944.950
D (5 MHz)	Cond. Valid	300–324	1865.000–1866.200	1945.000–1946.200
	Valid	325–375	1866.250–1868.750	1946.250–1948.750
	Cond. Valid	376–399	1868.800–1869.950	1948.800–1949.950
B (15 MHz)	Cond. Valid	400–424	1870.000–1871.200	1950.000–1951.200
	Valid	425–675	1871.250–1883.750	1951.250–1963.750
	Cond. Valid	676–699	1883.800–1884.950	1963.800–1964.950
E (5 MHz)	Cond. Valid	700–724	1885.000–1886.200	1965.000–1966.200
	Valid	725–775	1886.250–1888.750	1966.250–1968.750
	Cond. Valid	776–799	1888.800–1889.950	1968.800–1969.950
F (5 MHz)	Cond. Valid	800–824	1890.000–1891.200	1970.000–1971.200
	Valid	825–875	1891.250–1893.750	1971.250–1973.750
	Cond. Valid	876–899	1893.800–1894.950	1973.800–1974.950
C (15 MHz)	Cond. Valid	900–924	1895.000–1896.200	1975.000–1976.200
	Valid	925–1175	1896.250–1908.750	1976.250–1988.750
	Not Valid	1176–1199	1908.800–1909.950	1988.800–1989.950

3           **9.2.1.1.3 Band Class 2 (TACS Band)**

4           The Band Class 2 block designators for the access terminal and access network shall be as  
 5           specified in Table 9.2.1.1.1.3-1.

6           Access terminals supporting Band Class 2 shall be capable of transmitting in Band Class 2  
 7           using at least one band subclass. The band subclasses for Band Class 2 are specified in  
 8           Table 9.2.1.1.1.3-2.

9           The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 10          Band Class 2 shall be as specified in Table 9.2.1.1.1.3-3. Access terminals supporting Band  
       11          Class 2 shall support transmission on the valid and conditionally valid channel numbers  
       12          shown in Table 9.2.1.1.1.3-4. Transmission on the conditionally valid channels is  
       13          permissible if valid authorization has been obtained.

14          The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the  
       15          frequency of the access network transmit signal as measured at the access terminal  
       16          receiver.

**Table 9.2.1.1.3-1. Band Class 2 Block Frequency Correspondence**

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	872.0125–879.9875	917.0125–924.9875
	890.0125–897.4875	935.0125–942.4875
	905.0125–908.9875	950.0125–953.9875
B	880.0125–887.9875	925.0125–932.9875
	897.5125–904.9875	942.5125–949.9875
	909.0125–914.9875	954.0125–959.9875

**Table 9.2.1.1.3-2. Band Class 2 Band Subclasses**

Band Subclass	Number of Channels Covered	Channels Covered
0	600	1–600
1	1000	1–1000
2	1320	1329–2047 and 0–600

**Table 9.2.1.1.3-3. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 2**

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 1000$	$0.025 N + 889.9875$
	$1329 \leq N \leq 2047$	$0.025 (N - 1328) + 871.9875$
Access Network	$0 \leq N \leq 1000$	$0.025 N + 934.9875$
	$1329 \leq N \leq 2047$	$0.025 (N - 1328) + 916.9875$

1           **Table 9.2.1.1.3-4. CDMA Channel Numbers and Corresponding Frequencies**  
 2           **for Band Class 2**

<b>Block Designator</b>	<b>CDMA Channel Validity</b>	<b>CDMA Channel Number</b>	<b>Transmit Frequency Band (MHz)</b>	
			<b>Access Terminal</b>	<b>Access Network</b>
A ETACS (8 MHz)	Not Valid	1329–1355	872.0125–872.6625	917.0125–917.6625
	Valid-1320	1356–1648	872.6875–879.9875	917.6875–924.9875
B ETACS (8 MHz)	Valid-1320	1649–1941	880.0125–887.3125	925.0125–932.3125
	Cond. Valid-1320	1942–1968	887.3375–887.9875	932.3375–932.9875
Unassigned (2 MHz)	Cond. Valid-1320	1969–2047	888.0125–889.9625	933.0125–934.9625
		0	889.9875	934.9875
A (7.5 MHz)	Cond. Valid-1320	1–27	890.0125–890.6625	935.0125–935.6625
	Valid	28–300	890.6875–897.4875	935.6875–942.4875
B (7.5 MHz)	Valid	301–573	897.5125–904.3125	942.5125–949.3125
	Valid-1000	574–600	904.3375–904.9875	949.3375–949.9875
A'	Valid-1000	601–760	905.0125–908.9875	950.0125–953.9875
B' (6 MHz)	Valid-1000	761–973	909.0125–914.3125	954.0125–959.3125
	Not Valid	974–1000	914.3375–914.9875	959.3375–959.9875

Valid and Not Valid apply to the channels for the access terminals of all three band subclasses. Valid-1000 means that the channels are only valid for the access terminals of band subclass 1. Valid-1320 means that the channels are only valid for the access terminals of band subclass 2. Cond. Valid-1320 means that the channels are conditionally valid for the access terminals of band subclass 2, and that they are not valid for the access terminals of band subclasses 0 and 1.

3

#### 4           9.2.1.1.4 Band Class 3 (JTACS Band)

5           The Band Class 3 system designators for the access terminal and access network shall be  
 6           as specified in Table 9.2.1.1.4-1.

7           Access terminals supporting Band Class 3 shall be capable of transmitting in Band Class 3.

8           The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 9           Band Class 3 shall be as specified in Table 9.2.1.1.4-2. Access terminals supporting Band  
 10          Class 3 shall support transmission on the valid channel numbers shown in Table  
 11          9.2.1.1.4-3.

12          The nominal access terminal transmit carrier frequency shall be 55.0 MHz higher than the  
 13          frequency of the access network transmit signal as measured at the access terminal  
 14          receiver.

**Table 9.2.1.1.4-1. Band Class 3 System Frequency Correspondence**

<b>System Designator</b>	<b>Transmit Frequency Band (MHz)</b>	
	<b>Access Terminal</b>	<b>Access Network</b>
A	887.0125–888.9875	832.0125–833.9875
	893.0125–898.0000	838.0125–843.0000
	898.0125–900.9875	843.0125–845.9875
	915.0125–924.9875	860.0125–869.9875
B	Not specified	Not specified

**Table 9.2.1.1.4-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 3**

<b>Transmitter</b>	<b>CDMA Channel Number</b>	<b>Center Frequency for CDMA Channel (MHz)</b>
Access Terminal	$1 \leq N \leq 799$	$0.0125 N + 915.000$
	$801 \leq N \leq 1039$	$0.0125 (N - 800) + 898.000$
	$1041 \leq N \leq 1199$	$0.0125 (N - 1040) + 887.000$
	$1201 \leq N \leq 1600$	$0.0125 (N - 1200) + 893.000$
Access Network	$1 \leq N \leq 799$	$0.0125 N + 860.000$
	$801 \leq N \leq 1039$	$0.0125 (N - 800) + 843.000$
	$1041 \leq N \leq 1199$	$0.0125 (N - 1040) + 832.000$
	$1201 \leq N \leq 1600$	$0.0125 (N - 1200) + 838.000$

In this table, only even-valued N values are valid.

1           **Table 9.2.1.1.4-3. CDMA Channel Numbers and Corresponding Frequencies**  
 2           **for Band Class 3**

<b>System Designator</b>	<b>CDMA Channel Validity</b>	<b>CDMA Channel Number</b>	<b>Transmit Frequency Band (MHz)</b>	
			<b>Access Terminal</b>	<b>Access Network</b>
A1 (2 MHz)	Not Valid	1041–1099	887.0125–887.7375	832.0125–832.7375
	Valid	1100–1140	887.7500–888.2500	832.7500–833.2500
	Not Valid	1141–1199	888.2625–888.9875	833.2625–833.9875
A3 (5 MHz)	Not Valid	1201–1259	893.0125–893.7375	838.0125–838.7375
	Valid	1260–1540	893.7500–897.2500	838.7500–842.2500
	Cond. Valid	1541–1600	897.2625–898.0000	842.2625–843.0000
A2 (3 MHz)	Cond. Valid	801–859	898.0125–898.7375	843.0125–843.7375
	Valid	860–980	898.7500–900.2500	843.7500–845.2500
	Not Valid	981–1039	900.2625–900.9875	845.2625–845.9875
A (10 MHz)	Not Valid	1–59	915.0125–915.7375	860.0125–860.7375
	Valid	60–740	915.7500–924.2500	860.7500–869.2500
	Not Valid	741–799	924.2625–924.9875	869.2625–869.9875
B	Not specified	Not specified	Not specified	Not specified

3           **9.2.1.1.5 Band Class 4 (Korean PCS Band)**

4           The Band Class 4 block designators for the access terminal and access network shall be as  
 5           specified in Table 9.2.1.1.5-1.

6           Access terminals supporting Band Class 4 shall be capable of transmitting in Band Class 4.

7           The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 8           Band Class 4 shall be as specified in Table 9.2.1.1.5-2. Access terminals supporting Band  
 9           Class 4 shall support transmission on the valid and conditionally valid channel numbers  
 10          shown in Table 9.2.1.1.5-3. Transmission on conditionally valid channels is permissible if  
 11          the adjacent block is allocated to the same licensee or if other valid authorization has been  
 12          obtained.

13          The nominal access terminal transmit carrier frequency shall be 90.0 MHz lower than the  
 14          frequency of the access network transmit signal as measured at the access terminal  
 15          receiver.

**Table 9.2.1.1.5-1. Band Class 4 Block Frequency Correspondence**

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	1750–1760	1840–1850
B	1760–1770	1850–1860
C	1770–1780	1860–1870

**Table 9.2.1.1.5-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 4**

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 599$	0.050 N + 1750.000
Access Network	$0 \leq N \leq 599$	0.050 N + 1840.000

**Table 9.2.1.1.5-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 4**

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (10 MHz)	Not Valid	0–24	1750.000–1751.200	1840.000–1841.200
	Valid	25–175	1751.250–1758.750	1841.250–1848.750
	Cond. Valid	176–199	1758.800–1759.950	1848.800–1849.950
B (10 MHz)	Cond. Valid	200–224	1760.000–1761.200	1850.000–1851.200
	Valid	225–375	1761.250–1768.750	1851.250–1858.750
	Cond. Valid	376–399	1768.800–1769.950	1858.800–1859.950
C (10 MHz)	Cond. Valid	400–424	1770.000–1771.200	1860.000–1861.200
	Valid	425–575	1771.250–1778.750	1861.250–1868.750
	Not Valid	576–599	1778.800–1779.950	1868.800–1869.950

#### 9.2.1.1.6 Band Class 5 (450-MHz Band)

The Band Class 5 block designators for the access terminal and access network shall be as specified in Table 9.2.1.1.6-1.

There are eight band subclasses specified for Band Class 5. Each band subclass corresponds to a specific block designator (see Table 9.2.1.1.6-1). Each band subclass includes all the channels designated for that system. Access terminals supporting Band Class 5 shall be capable of transmitting in at least one band subclass belonging to Band Class 5. For access terminals capable of transmitting in more than one band subclass

- 1 belonging to Band Class 5, one band subclass shall be designated as the Primary Band  
 2 Subclass, which is the band subclass used by the access terminal's home system.
- 3 The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 4 Band Class 5 shall be as specified in Table 9.2.1.1.6-2. Access terminals supporting Band  
 5 Class 5 shall support transmission on the valid and conditionally valid channel numbers  
 6 shown in Table 9.2.1.1.6-3, depending on the Band Subclass of the access terminal. Note  
 7 that certain channel assignments in Block A are not valid and others are conditionally  
 8 valid. Transmission on conditionally valid channels is permissible if the adjacent A' block is  
 9 allocated to the same licensee or if other valid authorization has been obtained.
- 10 The nominal access terminal transmit carrier frequency shall be 10.0 MHz lower than the  
 11 frequency of the access network transmit signal as measured at the access terminal  
 12 receiver.

13 **Table 9.2.1.1.6-1. Band Class 5 Block Frequency Correspondence and Band**  
 14 **Subclasses**

<b>Block Designator</b>	<b>Band Subclass</b>	<b>Transmit Frequency Band (MHz)</b>	
		<b>Access Terminal</b>	<b>Access Network</b>
A	0	452.500–457.475	462.500–467.475
B	1	452.000–456.475	462.000–466.475
C	2	450.000–454.800	460.000–464.800
D	3	411.675–415.850	421.675–425.850
E	4	415.500–419.975	425.500–429.975
F	5	479.000–483.480	489.000–493.480
G	6	455.230–459.990	465.230–469.990
H	7	451.310–455.730	461.310–465.730

**Table 9.2.1.1.6-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 5**

<b>Transmitter</b>	<b>CDMA Channel Number</b>	<b>Center Frequency for CDMA Channel (MHz)</b>
Access Terminal	$1 \leq N \leq 300$	$0.025(N - 1) + 450.000$
	$539 \leq N \leq 871$	$0.025(N - 512) + 411.000$
	$1039 \leq N \leq 1473$	$0.020(N - 1024) + 451.010$
	$1792 \leq N \leq 2016$	$0.020(N - 1792) + 479.000$
Access Network	$1 \leq N \leq 300$	$0.025(N - 1) + 460.000$
	$539 \leq N \leq 871$	$0.025(N - 512) + 421.000$
	$1039 \leq N \leq 1473$	$0.020(N - 1024) + 461.010$
	$1792 \leq N \leq 2016$	$0.020(N - 1792) + 489.000$

3

1           **Table 9.2.1.1.6-3. CDMA Channel Numbers and Corresponding Frequencies**  
 2           **for Band Class 5**

<b>Block Designator</b>	<b>CDMA Channel Validity</b>	<b>CDMA Channel Number</b>	<b>Transmit Frequency Band (MHz)</b>	
			<b>Access Terminal</b>	<b>Access Network</b>
A (4.5 MHz)	Not Valid	121–125	453.000–453.100	463.000–463.100
	Cond. Valid	126–145	453.125–453.600	463.125–463.600
	Valid	146–275	453.625–456.850	463.625–466.850
	Not Valid	276–300	456.875–457.475	466.875–467.475
A' (0.5 MHz)	Not Valid	101–120	452.500–452.975	462.500–462.975
B (4.5 MHz)	Not Valid	81–105	452.000–452.600	462.000–462.600
	Valid	106–235	452.625–455.850	462.625–465.850
	Not Valid	236–260	455.875–456.475	465.875–466.475
C (4.8 MHz)	Not Valid	1–25	450.000–450.600	460.000–460.600
	Valid	26–168	450.625–454.175	460.625–464.175
	Not Valid	169–193	454.200–454.800	464.200–464.800
D (4.2 MHz)	Not Valid	539–563	411.675–412.275	421.675–422.275
	Valid	564–681	412.300–415.225	422.300–425.225
	Not Valid	682–706	415.250–415.850	425.250–425.850
E (4.5 MHz)	Not Valid	692–716	415.500–416.100	425.500–426.100
	Valid	717–846	416.125–419.350	426.125–429.350
	Not Valid	847–871	419.375–419.975	429.375–429.975
F (4.5 MHz)	Not Valid	1792–1822	479.000–479.600	489.000–489.600
	Valid	1823–1985	479.620–482.860	489.620–492.860
	Not Valid	1986–2016	482.880–483.480	492.880–493.480
G (4.76 MHz)	Not Valid	1235–1265	455.230–455.830	465.230–465.830
	Valid	1266–1442	455.850–459.370	465.850–469.370
	Not Valid	1443–1473	459.390–459.990	469.390–469.990
H (4.42 MHz)	Not Valid	1039–1069	451.310–451.910	461.310–461.910
	Valid	1070–1229	451.930–455.110	461.930–465.110
	Not Valid	1230–1260	455.130–455.730	465.130–465.730

3

## 4           9.2.1.1.7 Band Class 6 (2-GHz Band)

5           The Band Class 6 block designators for the access terminal and access network are not  
 6           specified, since licensee allocations vary by regulatory body.

7           Access terminals supporting Band Class 6 shall be capable of transmitting in Band Class 6.

8           The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 9           Band Class 6 shall be as specified in Table 9.2.1.1.7-1. Access terminals supporting Band

1 Class 6 shall support transmission on the valid channel numbers shown in Table  
 2 9.2.1.1.7-2.

3 The nominal access terminal transmit carrier frequency shall be 190.0 MHz lower than the  
 4 frequency of the access network transmit signal as measured at the access terminal  
 5 receiver.

6 **Table 9.2.1.1.7-1. CDMA Channel Number to CDMA Frequency Assignment**  
 7 **Correspondence for Band Class 6**

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 1199$	$1920.000 + 0.050 N$
Access Network	$0 \leq N \leq 1199$	$2110.000 + 0.050 N$

9 **Table 9.2.1.1.7-2. CDMA Channel Numbers and Corresponding Frequencies**  
 10 **for Band Class 6**

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	1920.000–1921.200	2110.000–2111.200
Valid	25–1175	1921.250–1978.750	2111.250–2168.750
Not Valid	1176–1199	1978.800–1979.950	2168.800–2169.950

11 Channel numbers less than 1.25 MHz from the licensee's band edge  
 are not valid.

#### 12 9.2.1.1.8 Band Class 7 (700-MHz Band)

13 The Band Class 7 block designators for the access terminal and access network shall be as  
 14 specified in Table 9.2.1.1.8-1.

15 Access terminals supporting Band Class 7 shall be capable of transmitting in Band Class 7.

16 The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 17 Band Class 7 shall be as specified in Table 9.2.1.1.8-2. Access terminals supporting Band  
 18 Class 7 shall support operations on the valid and conditionally valid channel numbers  
 19 shown in Table 9.2.1.1.8-3. Note that certain channel assignments are not valid and  
 20 others are conditionally valid. Transmission on conditionally valid channels is permissible if  
 21 the adjacent block is allocated to the same licensee or if other valid authorization has been  
 22 obtained.

23 The nominal access terminal transmit carrier frequency shall be 30.0 MHz higher than the  
 24 frequency of the access network transmit signal as measured at the access terminal  
 25 receiver.

**Table 9.2.1.1.8-1. Band Class 7 Block Frequency Correspondence**

Block Designator	Transmit Frequency Band (MHz)	
	Access Terminal	Access Network
A	776–777	746–747
C	777–782	747–752
D	782–792	752–762
B	792–794	762–764

**Table 9.2.1.1.8-2. CDMA Channel Number to CDMA Frequency Assignment Correspondence for Band Class 7**

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 359$	$776.000 + 0.050 N$
Access Network	$0 \leq N \leq 359$	$746.000 + 0.050 N$

**Table 9.2.1.1.8-3. CDMA Channel Numbers and Corresponding Frequencies for Band Class 7**

Block Designator	CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
			Access Terminal	Access Network
A (1 MHz)	Not Valid	0–19	776.000–776.950	746.000–746.950
C (5 MHz)	Not Valid	20–44	777.000–778.200	747.000–748.200
	Valid	45–95	778.250–780.750	748.250–750.750
	Cond. Valid	96–119	780.800–781.950	750.800–751.950
D (10 MHz)	Cond. Valid	120–144	782.000–783.200	752.000–753.200
	Valid	145–295	783.250–790.750	753.250–760.750
	Not Valid	296–319	790.800–791.950	760.800–761.950
B (2 MHz)	Not Valid	320–359	792.000–793.950	762.000–763.950

**9.2.1.1.9 Band Class 8 (1800-MHz Band)**

The Band Class 8 block designators for the access terminal and the access network are not specified.

Access terminals supporting Band Class 8 shall be capable of transmitting in Band Class 8.

- 1 The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 2 Band Class 8 shall be as specified in Table 9.2.1.1.9-1. Access terminals supporting Band  
 3 Class 8 shall support transmission on the valid channel numbers shown in Table  
 4 9.2.1.1.9-2.
- 5 The nominal access terminal transmit carrier frequency shall be 95.0 MHz lower than the  
 6 frequency of the access network transmit signal as measured at the access terminal  
 7 receiver.

8 **Table 9.2.1.1.9-1. CDMA Channel Number to CDMA Frequency Assignment**  
 9 **Correspondence for Band Class 8**

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 1499$	$1710.000 + 0.050 N$
Access Network	$0 \leq N \leq 1499$	$1805.000 + 0.050 N$

10

11 **Table 9.2.1.1.9-2. CDMA Channel Numbers and Corresponding Frequencies for Band**  
 12 **Class 8**

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	1710.000–1711.200	1805.000–1806.200
Valid	25–1475	1711.250–1783.750	1806.250–1878.750
Not Valid	1476–1499	1783.800–1784.950	1878.800–1879.950

Channel numbers less than 1.25 MHz from the licensee's band edge  
 are not valid.

13

14 9.2.1.1.10 Band Class 9 (900-MHz Band)

15 The Band Class 9 block designators for the access terminal and the access network are not  
 16 specified.

17 Access terminals supporting Band Class 9 shall be capable of transmitting in Band Class 9.

18 The channel spacing, CDMA channel designations, and transmitter center frequencies of  
 19 Band Class 9 shall be as specified in Table 9.2.1.1.10-1. Access terminals supporting  
 20 Band Class 9 shall support transmission on the valid channel numbers shown Table  
 21 9.2.1.1.10-2.

22 The nominal access terminal transmit carrier frequency shall be 45.0 MHz lower than the  
 23 frequency of the access network transmit signal as measured at the access terminal  
 24 receiver.

1           **Table 9.2.1.1.10-1. CDMA Channel Number to CDMA Frequency Assignment**  
 2           Correspondence for Band Class 9

Transmitter	CDMA Channel Number	Center Frequency for CDMA Channel (MHz)
Access Terminal	$0 \leq N \leq 699$	$880.000 + 0.050 N$
Access Network	$0 \leq N \leq 699$	$925.000 + 0.050 N$

3  
 4           **Table 9.2.1.1.10-2. CDMA Channel Numbers and Corresponding Frequencies for**  
 5           **Band Class 9**

CDMA Channel Validity	CDMA Channel Number	Transmit Frequency Band (MHz)	
		Access Terminal	Access Network
Not Valid	0–24	880.000–881.200	925.000–926.200
Valid	25–675	881.250–913.750	926.250–958.750
Not Valid	676–699	913.800–914.950	958.800–959.950

Channel numbers less than 1.25 MHz from the licensee's band edge  
 are not valid.

6  
 7           9.2.1.1.2 Frequency Tolerance

8           The access terminal shall meet the requirements in the current version of [5].

9           9.2.1.2 Power Output Characteristics

10          All power levels are referenced to the access terminal antenna connector unless otherwise  
 11        specified.

12          9.2.1.2.1 Output Power Requirements of Reverse Channels

13          9.2.1.2.1.1 Access Channel Output Power

14          When transmitting over the Access Channel, the access terminal transmits Access Probes  
 15        until the access attempt succeeds or ends.

16          9.2.1.2.1.2 Reverse Traffic Channel Output Power

17          When the access terminal is transmitting the Reverse Traffic Channel, the access terminal  
 18        shall control the mean output power using a combination of closed-loop and open-loop  
 19        power control (see 9.2.1.2.4 and 9.2.1.4). Throughout 9.2.1.2, the channel formed by  
 20        multiplexing the RRI Channel onto the Pilot Channel is still referred to as the Pilot Channel.

21          When the access terminal is transmitting the Reverse Traffic Channel, the access terminal  
 22        transmits the Pilot Channel, the DRC Channel, the ACK Channel when acknowledging  
 23        received physical layer packets, and the Data Channel when transmitting physical layer

1 packets. These channels shall be transmitted at power levels according to open-loop and  
2 closed-loop power control. The transmitted power level of the Data Channel shall be  
3 adjusted depending on the selected data rate (see 9.2.1.2.4) and reverse link power control.  
4 The traffic data shall be transmitted in the form of physical layer packets (duration 26.66...  
5 ms), which may occur either contiguously or sporadically. When the data rate is changed,  
6 the access terminal output power, relative to the desired value in steady state, shall be  
7 within  $\pm 0.5$  dB or 20% of the change in dB, whichever is greater. The access terminal  
8 output power shall settle to within  $\pm 0.5$  dB of the steady-state value within 200  $\mu$ s of the  
9 physical layer packet boundary.

10 9.2.1.2.2 Maximum Output Power

11 The access terminal shall meet the requirements in the current version of [5].

12 9.2.1.2.3 Output Power Limits

13 9.2.1.2.3.1 Minimum Controlled Output Power

14 The access terminal shall meet the requirements in the current version of [5].

15 9.2.1.2.3.2 Standby Output Power

16 The access terminal shall disable its transmitter except when it is instructed by a MAC  
17 protocol to transmit. When the transmitter is disabled, the output noise power spectral  
18 density of the access terminal shall be less than  $-61$  dBm/1 MHz for all frequencies within  
19 the transmit bands that the access terminal supports.

20 9.2.1.2.4 Controlled Output Power

21 The access terminal shall provide two independent means for output power adjustment: an  
22 open-loop estimation performed by the access terminal and a closed-loop correction  
23 involving both the access terminal and the access network. Accuracy requirements on the  
24 controlled range of mean output power (see 9.2.1.2.5) need not apply for the following three  
25 cases:

- 26 • Mean output power levels exceeding the minimum ERP/EIRP at the maximum  
27 output power for the corresponding access terminal class;
- 28 • Mean output power levels less than the minimum controlled output power (see  
29 9.2.1.2.3.1); or
- 30 • Mean input power levels exceeding  $-25$  dBm within the 1.23-MHz bandwidth.

31 9.2.1.2.4.1 Estimated Open-Loop Output Power

32 Open-loop operation shall be based on the power of the received Forward Pilot Channel (see  
33 9.3.1.3.2.1).

34 The nominal access probe structure and its transmit power requirements are defined as  
35 part of the Access Channel MAC Protocol. The power of the Access Data Channel relative to  
36 that of the Pilot Channel shall be as specified in Table 9.2.1.2.4.1-1 in which  
37 DataOffsetNom and DataOffset9k6 are public data of the Access Channel MAC Protocol. The

1 output power of the Pilot Channel during the preamble portion of an access probe shall be  
2 increased relative to the nominal Pilot Channel power during the data portion of the probe  
3 by an amount such that the total output power of the preamble and data portions of the  
4 access probe are the same.

5 Once instructed by the Reverse Traffic Channel MAC Protocol, the access terminal initiates  
6 Reverse Traffic Channel transmission. The initial mean output power of the Pilot Channel of  
7 the Reverse Traffic Channel shall be equal to the mean output power of the Pilot Channel at  
8 the end of the last Access Channel probe minus the difference in the forward link mean  
9 received signal power from the end of the last Access Channel probe to the start of the  
10 Reverse Traffic Channel transmission.

11 The subsequent mean output power of the Pilot Channel of the total reverse link  
12 transmission shall be as specified in 9.2.1.2.4.2.

13 The accuracy of the incremental adjustment to the mean output power, as dictated by the  
14 Access Channel MAC Protocol and the Reverse Traffic Channel MAC Protocol, shall be  
15  $\pm 0.5$  dB or 20% of the change (in dB), whichever is greater.

16 The access terminal shall support a total combined range of initial offset parameters, access  
17 probe corrections, and closed-loop power control corrections, of at least  $\pm 32$  dB for access  
18 terminals operating in Band Classes 0, 2, 3, 5, and 7 and  $\pm 40$  dB for access terminals  
19 operating in Band Classes 1, 4, and 6.

20 Prior to the application of access probe corrections and closed-loop power control  
21 corrections, the access terminal's open-loop mean output power of the Pilot Channel,  $X_0$ ,  
22 should be within  $\pm 6$  dB and shall be within  $\pm 9$  dB of the value given by

$$23 \quad X_0 = -\text{Mean Received Power (dBm)} + \text{OpenLoopAdjust} + \text{ProbeInitialAdjust}$$

24 where OpenLoopAdjust and ProbeInitialAdjust are public data from the Access Channel  
25 MAC Protocol and OpenLoopAdjust + ProbeInitialAdjust is from  $-81$  to  $-66$  dB for Band  
26 Classes 0, 2, 3, 5, and 7 and from  $-100$  to  $-69$  dB for Band Classes 1, 4, and 6.

27 During the transmission of the Reverse Traffic Channel, the determination of the output  
28 power needed to support the Data Channel, the DRC Channel, and the ACK Channel is an  
29 additional open-loop process performed by the access terminal.

30 The power of the Data Channel relative to that of the Pilot Channel shall be as specified in  
31 Table 9.2.1.2.4.1-1 in which DataOffsetNom, DataOffset9k6, DataOffset19k2,  
32 DataOffset38k4, DataOffset76k8, and DataOffset153k6 are public data of the Reverse  
33 Traffic Channel MAC Protocol.

**Table 9.2.1.2.4.1-1. Relative Power Levels vs. Data Rate**

<b>Data Rate (kbps)</b>	<b>Data Channel Gain Relative to Pilot (dB)</b>
0	$-\infty$ (Data Channel Is Not Transmitted)
9.6	DataOffsetNom + DataOffset9k6 + 3.75
19.2	DataOffsetNom + DataOffset19k2 + 6.75
38.4	DataOffsetNom + DataOffset38k4 + 9.75
76.8	DataOffsetNom + DataOffset76k8 + 13.25
153.6	DataOffsetNom + DataOffset153k6 + 18.5

During the transmission of the DRC Channel, the power of the DRC Channel relative to that of the Pilot Channel shall be as specified by DRCChannelGain, where DRCChannelGain is public data of the Forward Traffic Channel MAC Protocol.

During the transmission of the ACK Channel, the power of the ACK Channel relative to that of the Pilot Channel shall be as specified by ACKChannelGain, where ACKChannelGain is public data of the Forward Traffic Channel MAC Protocol.

The access terminal shall maintain the power of the Data Channel, DRC Channel and ACK Channel, relative to that of the Pilot Channel, to within  $\pm 0.25$  dB of the specified values.

If the access terminal is unable to transmit at the requested output power level when the maximum Reverse Traffic Channel data rate is 9600 bps, the access terminal shall reduce the power of the DRC Channel and the ACK Channel accordingly. The maximum power reduction for the DRC Channel corresponds to gating off the DRC Channel. The maximum power reduction for the ACK Channel corresponds to gating off the ACK Channel. If the ACK Channel is active, the ACK Channel power reduction shall occur only after the DRC Channel has been gated off. The access terminal shall perform the power reduction within one slot of determining that the access terminal is unable to transmit at the requested output power level.

#### 9.2.1.2.4.2 Closed-Loop Output Power

For closed-loop correction (with respect to the open-loop estimate), the access terminal shall adjust the mean output power level of the Pilot Channel in response to each power-control bit received on the Reverse Power Control (RPC) Channel. The nominal change in mean output power level of the Pilot Channel per single power-control bit shall be set according to the RPCStep public data of the Reverse Traffic Channel MAC Protocol.

For the 1.0 dB step size, the change in mean output power level per power-control bit shall be within  $\pm 0.5$  dB of the nominal value (1 dB), and the change in mean output power level per 10 power-control bits of the same sign shall be within  $\pm 2.0$  dB of 10 times the nominal change (10 dB). For the 0.5 dB step size, the change in mean output power level per power-control bit shall be within  $\pm 0.3$  dB of the nominal value (0.5 dB), and the change in mean output power level per 20 power-control bits of the same sign shall be within  $\pm 2.5$  dB of 20

1 times the nominal change (10 dB). A '0' power-control bit requires the access terminal to  
 2 increase transmit power, and a '1' power-control bit requires the access terminal to  
 3 decrease transmit power. The access terminal shall provide a closed-loop adjustment range  
 4 greater than  $\pm 24$  dB around its open-loop estimate.

5 See 9.2.1.4 for combining power-control bits received from different multipath components  
 6 or from different sectors during handoff.

7 9.2.1.2.5 Power Transition Characteristics

8 9.2.1.2.5.1 Open-Loop Estimation

9 Following a step change in mean input power,  $\Delta P_{in}$ , the mean output power of the access  
 10 terminal shall transition to its final value in a direction opposite in sign to  $\Delta P_{in}$ , with  
 11 magnitude contained between the mask limits defined by<sup>42</sup>:

- 12 • Upper Limit:

13 For  $0 < t < 24$  ms:  $\max [1.2 \times |\Delta P_{in}| \times (t/24), |\Delta P_{in}| \times (t/24) + 2.0 \text{ dB}] + 1.5 \text{ dB}$

14 For  $t \geq 24$  ms:  $\max [1.2 \times |\Delta P_{in}|, |\Delta P_{in}| + 0.5 \text{ dB}] + 1.5 \text{ dB}$

- 15 • Lower Limit:

16 For  $t > 0$ :  $\max [0.8 \times |\Delta P_{in}| \times [1 - e^{(1.66...-t)/36}] - 2.0 \text{ dB}, 0] - 1 \text{ dB}$

17 where "t" is expressed in units of milliseconds and  $\Delta P_{in}$  is expressed in units of dB.

18 These limits shall apply to a step change  $\Delta P_{in}$  of  $\pm 20$  dB or less. The absolute value of the  
 19 change in mean output power due to open-loop power control shall be a monotonically  
 20 increasing function of time. If the change in mean output power consists of discrete  
 21 increments, no single increment shall exceed 1.2 dB.

22 9.2.1.2.5.2 Closed-Loop Correction

23 Following the reception of a closed-loop power-control bit, the mean output power of the  
 24 access terminal shall be within 0.3 dB and 0.15 dB of the final value in less than 500  $\mu\text{s}$  for  
 25 step sizes of 1.0 dB and 0.5 dB, respectively.

26 9.2.1.3 Modulation Characteristics

27 9.2.1.3.1 Reverse Channel Structure

28 The Reverse Channel consists of the Access Channel and the Reverse Traffic Channel. The  
 29 Access Channel shall consist of a Pilot Channel and a Data Channel. The Reverse Traffic  
 30 Channel shall consist of a Pilot Channel, a Reverse Rate Indicator (RRI) Channel, a Data  
 31 Rate Control (DRC) Channel, an Acknowledgement (ACK) Channel, and a Data Channel.  
 32 The RRI Channel is used to indicate the data rate of the Data Channel being transmitted on  
 33 the Reverse Traffic Channel. The DRC Channel is used by the access terminal to indicate to  
 34 the access network the requested Forward Traffic Channel data rate and the selected

---

42 The mask limits allow for the effect of alternating closed-loop power-control bits.

1 serving sector on the Forward Channel. The ACK Channel is used by the access terminal to  
2 inform the access network whether or not the physical layer packet transmitted on the  
3 Forward Traffic Channel has been received successfully.

4 The structure of the reverse link channels for the Access Channel shall be as shown in  
5 Figure 9.2.1.3.1-1, and the structure of the reverse link channels for the Reverse Traffic  
6 Channel shall be as shown in Figure 9.2.1.3.1-2 and Figure 9.2.1.3.1-3. For the Reverse  
7 Traffic Channel, the encoded RRI Channel symbols shall be time-division multiplexed with  
8 the Pilot Channel. This time-division-multiplexed channel is still referred to as the Pilot  
9 Channel. For the Access Channel, the RRI symbols shall not be transmitted and the Pilot  
10 Channel shall not be time-division multiplexed. The Pilot Channel, the DRC Channel, the  
11 ACK Channel, and the Data Channel shall be orthogonally spread by Walsh functions of  
12 length 4, 8, or 16 (see 9.2.1.3.7). Each Reverse Traffic Channel shall be identified by a  
13 distinct user long code. The Access Channel for each sector shall be identified by a distinct  
14 Access Channel long code.

15 The Access Channel frame and Reverse Traffic Channel frame shall be 26.66... ms in  
16 duration and the frame boundary shall be aligned to the rollover of the short PN codes (see  
17 9.2.1.3.8.1). Each frame shall consist of 16 slots, with each slot 1.66... ms in duration.  
18 Each slot contains 2048 PN chips.

19 When the access terminal is transmitting a Reverse Traffic Channel, it shall continuously  
20 transmit the Pilot Channel and the RRI Channel. These channels shall be time-division  
21 multiplexed, and shall be transmitted on Walsh channel  $W_0^{16}$ . When the DRC Channel is  
22 active (see 9.2.1.3.3.3), it shall be transmitted for full slot durations on Walsh channel  
23  $W_8^{16}$ . The access terminal shall transmit an ACK Channel bit in response to every Forward  
24 Traffic Channel slot that is associated with a detected preamble directed to the access  
25 terminal. Otherwise, the ACK Channel shall be gated off. When the ACK Channel bit is  
26 transmitted, it shall be transmitted on the first half slot on Walsh channel  $W_4^8$ .

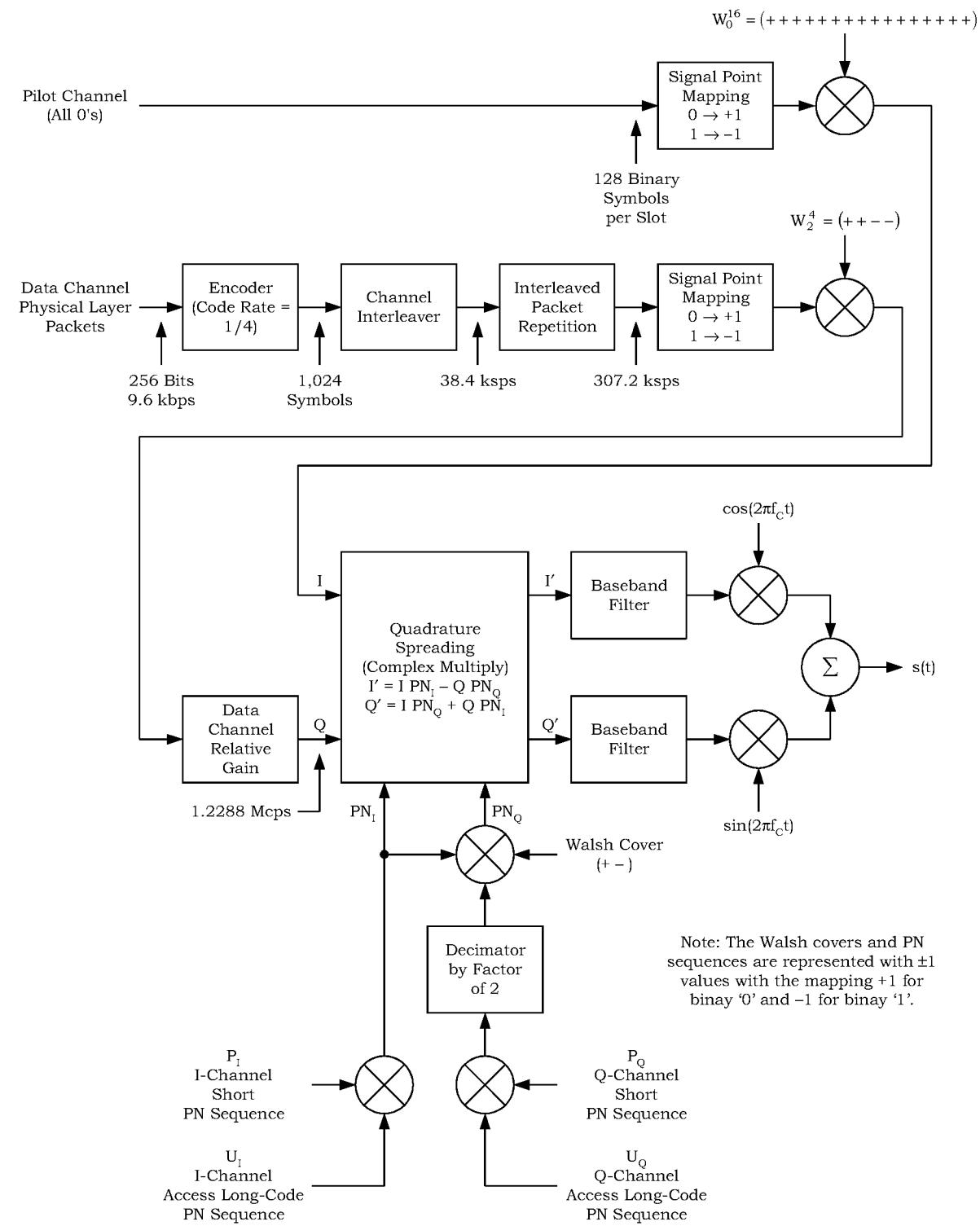
27 For the Reverse Traffic Channel, the encoded RRI symbols shall be time-division  
28 multiplexed with the Pilot Channel, and the encoded RRI symbols shall be allocated the first  
29 256 chips of every slot as shown in Figure 9.2.1.3.1-4.

30 Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6 give examples of the ACK Channel operation for a  
31 153.6-kbps Forward Traffic Channel. The 153.6-kbps Forward Traffic Channel physical  
32 layer packets use four slots, and these slots are transmitted with a three-slot interval  
33 between them, as shown in the figures. The slots from other physical layer packets are  
34 interlaced in the three intervening slots.

35 Figure 9.2.1.3.1-5 shows the case of a normal physical layer packet termination. In this  
36 case, the access terminal transmits NAK responses on the ACK Channel after the first three  
37 slots of the physical layer packet are received indicating that it was unable to correctly  
38 receive the Forward Traffic Channel physical layer packet after only one, two, or three of the  
39 nominal four slots. An ACK or NAK is also transmitted after the last slot is received, as  
40 shown.

- 1 Figure 9.2.1.3.1-6 shows the case where the Forward Traffic Channel physical layer packet  
2 transmission is terminated early. In this example, the access terminal transmits an ACK  
3 response on the ACK Channel after the third slot is received indicating that it has correctly  
4 received the physical layer packet. When the access network receives such an ACK  
5 response, it does not transmit the remaining slots of the physical layer packet. Instead, it  
6 may begin transmission of any subsequent physical layer packets.
- 7 When the access terminal has received all slots of a physical layer packet or has  
8 transmitted a positive ACK response, the physical layer shall return a  
9 *ForwardTrafficCompleted* indication.

10



1

2

**Figure 9.2.1.3.1-1. Reverse Channel Structure for the Access Channel**

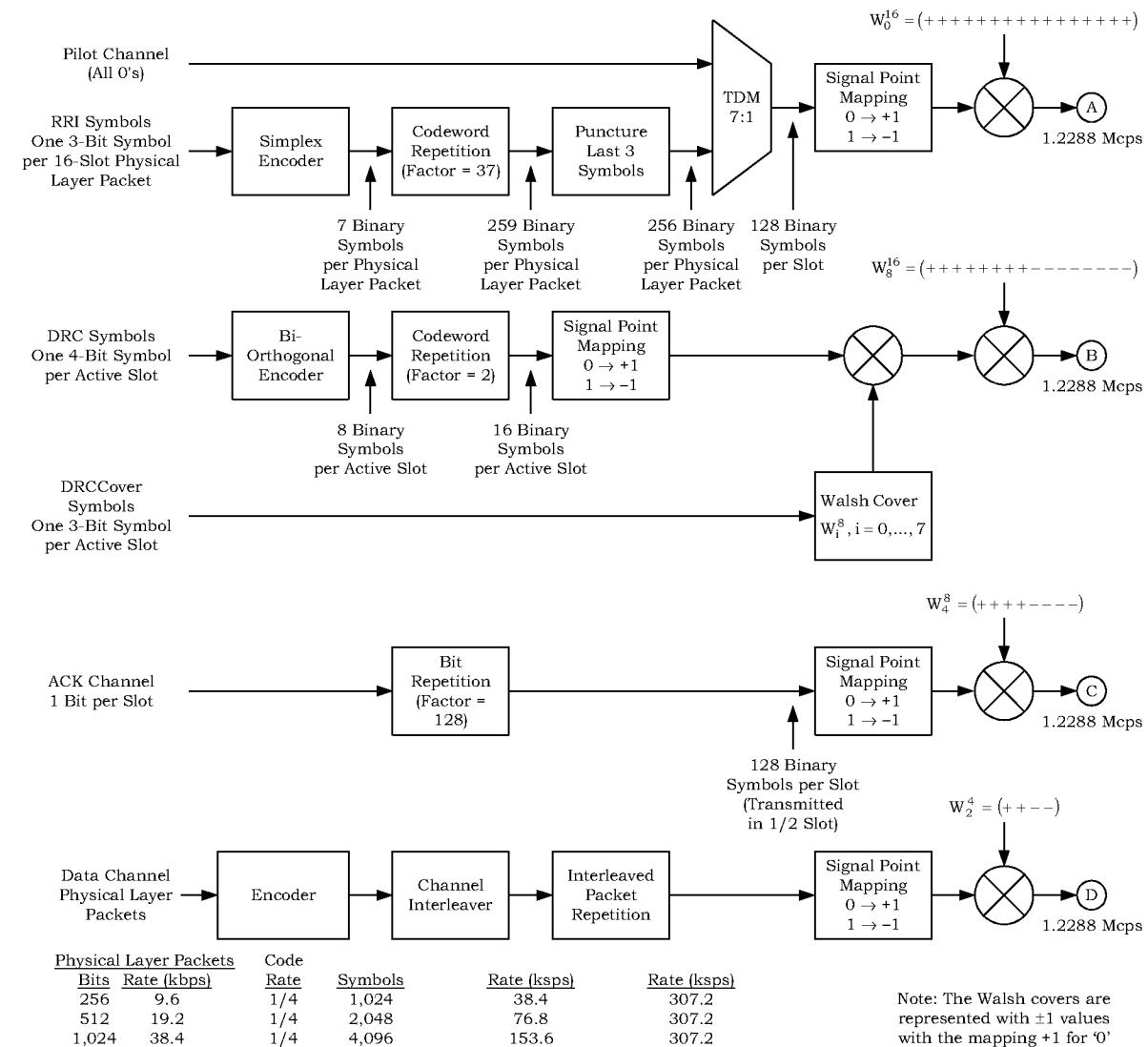
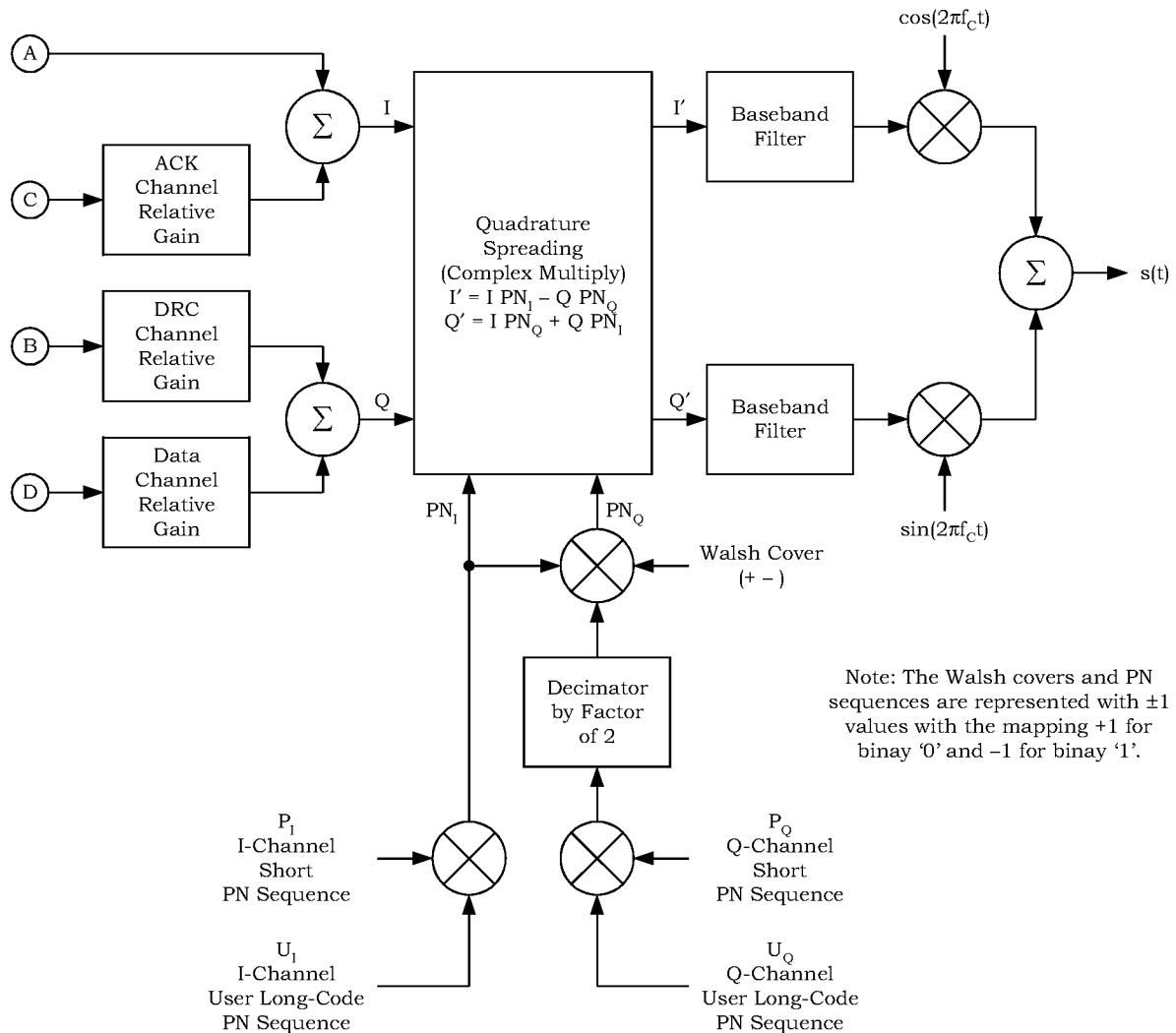
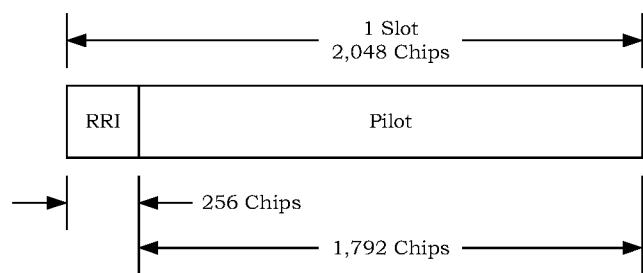


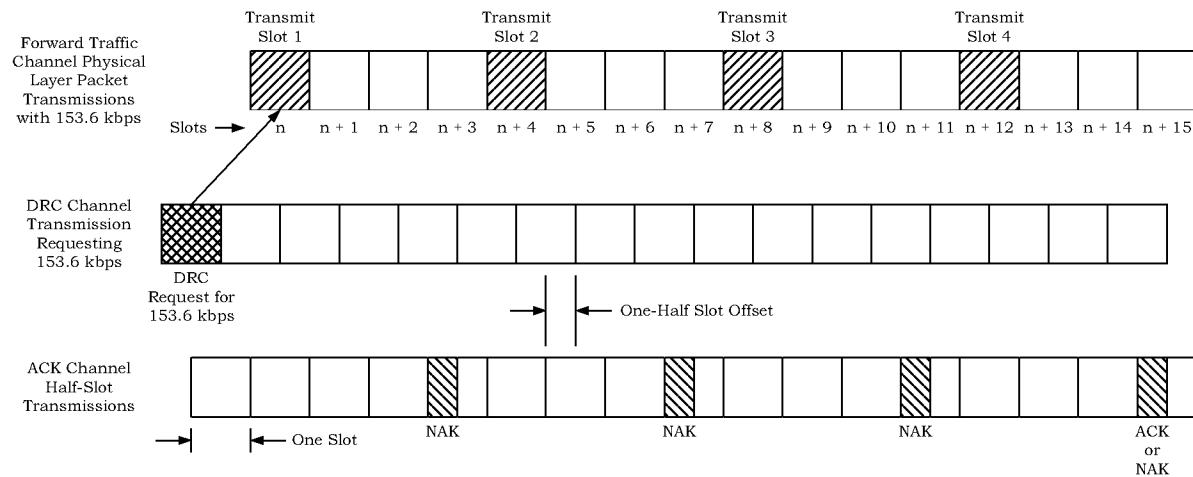
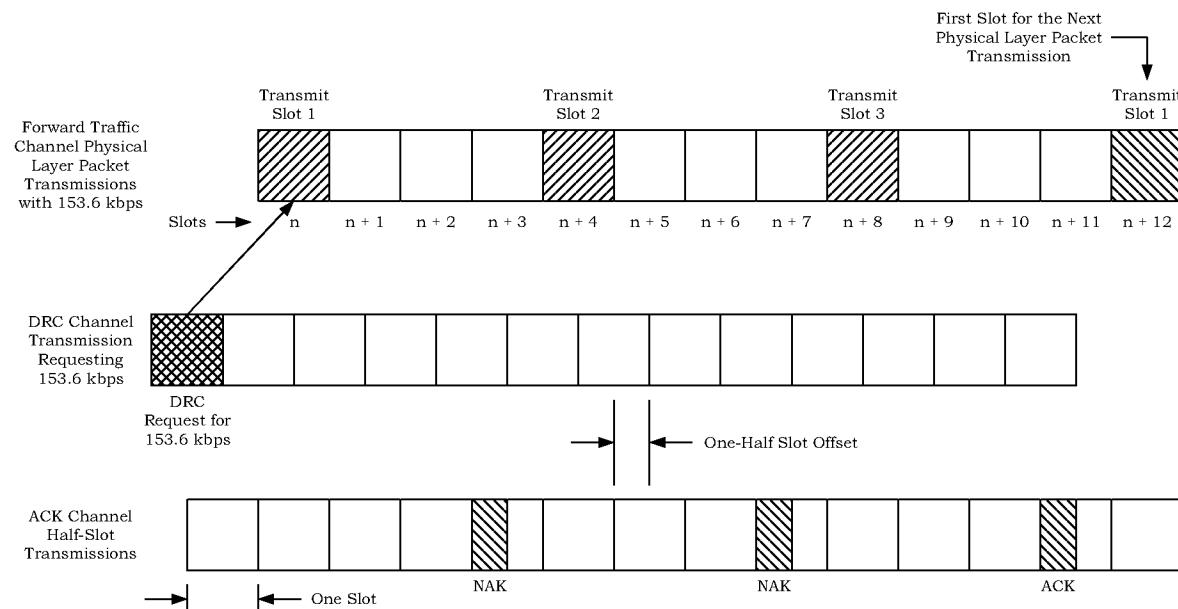
Figure 9.2.1.3.1-2. Reverse Channel Structure for the Reverse Traffic Channel  
(Part 1 of 2)



**Figure 9.2.1.3.1-3. Reverse Channel Structure for the Reverse Traffic Channel (Part 2 of 2)**



**Figure 9.2.1.3.1-4. Pilot Channel and RRI Channel TDM Allocations for the Reverse Traffic Channel**

**Figure 9.2.1.3.1-5. Multislot Physical Layer Packet with Normal Termination****Figure 9.2.1.3.1-6. Multislot Physical Layer Packet with Early Termination**

## 5    9.2.1.3.1.1 Modulation Parameters

6    The modulation parameters for the Access Channel and the Reverse Traffic Channel shall  
 7    be as specified in Table 9.2.1.3.1.1-1.

1      **Table 9.2.1.3.1.1-1. Modulation Parameters for the Access Channel and the Reverse**  
 2      **Traffic Channel**

<b>Parameter</b>	<b>Data Rate (kbps)</b>				
	<b>9.6</b>	<b>19.2</b>	<b>38.4</b>	<b>76.8</b>	<b>153.6</b>
Reverse Rate Index	1	2	3	4	5
Bits per Physical Layer Packet	256	512	1,024	2,048	4,096
Physical Layer Packet Duration (ms)	26.66...	26.66...	26.66...	26.66...	26.66...
Code Rate	1/4	1/4	1/4	1/4	1/2
Code Symbols per Physical Layer Packet	1,024	2,048	4,096	8,192	8,192
Code Symbol Rate (ksps)	38.4	76.8	153.6	307.2	307.2
Interleaved Packet Repeats	8	4	2	1	1
Modulation Symbol Rate (ksps)	307.2	307.2	307.2	307.2	307.2
Modulation Type	BPSK	BPSK	BPSK	BPSK	BPSK
PN Chips per Physical Layer Packet Bit	128	64	32	16	8

3      4      **9.2.1.3.1.2 Data Rates**

5      The access terminal shall transmit information on the Access Channel at a fixed data rate  
 6      of 9.6 kbps.

7      The access terminal shall transmit information on the Reverse Traffic Channel at a variable  
 8      data rate of 9.6, 19.2, 38.4, 76.8, or 153.6 kbps, according to the Reverse Traffic Channel  
 9      MAC Protocol.

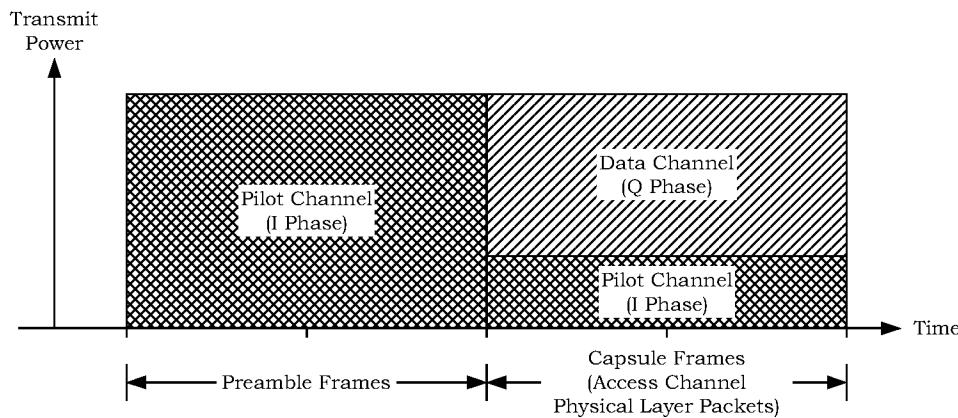
10     **9.2.1.3.2 Access Channel**

11     The Access Channel is used by the access terminal to initiate communication with the  
 12     access network or to respond to an access terminal directed message. The Access Channel  
 13     consists of a Pilot Channel and a Data Channel as shown in Figure 9.2.1.3.1-1.

14     An access probe shall consist of a preamble followed by one or more Access Channel  
 15     physical layer packets. During the preamble transmission, only the Pilot Channel is  
 16     transmitted. During the Access Channel physical layer packet transmission, both the Pilot

1 Channel and the Data Channel are transmitted. The output power of the Pilot Channel  
 2 during the preamble portion of an access probe is higher than it is during the data portion  
 3 of the probe by an amount such that the total output power of the preamble and data  
 4 portions of the access probe are the same as shown in Figure 9.2.1.3.2-1.

5 The preamble length is specified by the parameter PreambleLength which is public data  
 6 from the Access Channel MAC Protocol. The Access Channel physical layer packets are  
 7 transmitted at a fixed data rate of 9.6 kbps.



**Figure 9.2.1.3.2-1. Example of an Access Probe**

#### 9.2.1.3.2.1 Pilot Channel

11 The access terminal shall transmit unmodulated symbols with a binary value of '0' on the  
 12 Pilot Channel. The Pilot Channel shall be transmitted continuously during Access Channel  
 13 transmission. It shall be transmitted on the I channel using the 16-chip Walsh function  
 14 number 0 ( $W_0^{16} = + + + + + + + + + + + + + + + +$ ) cover.

#### 9.2.1.3.2.2 Data Channel

16 One or more Access Channel physical layer packets shall be transmitted on the Data  
 17 Channel during every access probe. The Access Channel physical layer packets shall be  
 18 transmitted at a fixed data rate of 9.6 kbps on the Q channel using the 4-chip Walsh  
 19 function number 2 ( $W_2^4 = + + - -$ ). The Access Channel physical layer packets shall be  
 20 preceded by a preamble of PreambleLength frames where only the Pilot Channel is  
 21 transmitted. The PreambleLength parameter is public data from the Access Channel MAC  
 22 Protocol.

#### 9.2.1.3.3 Reverse Traffic Channel

24 The Reverse Traffic Channel is used by the access terminal to transmit user-specific traffic  
 25 or signaling information to the access network. The Reverse Traffic Channel consists of a  
 26 Pilot Channel, an RRI Channel, a DRC Channel, an ACK Channel, and a Data Channel.

27 The access terminal shall support transmission of information on the Data Channel of the  
 28 Reverse Traffic Channel at data rates of 9.6, 19.2, 38.4, 76.8, and 153.6 kbps. The data  
 29 rate used on the Data Channel is specified by the Reverse Traffic Channel MAC Protocol.

1 The gain of the Data Channel relative to that of the Pilot Channel for the Reverse Traffic  
 2 Channel depends on the data rate as shown in Table 9.2.1.2.4.1-1.

3 9.2.1.3.3.1 Pilot Channel

4 The access terminal shall transmit unmodulated symbols with a binary value of '0' on the  
 5 Pilot Channel. The transmission of the Pilot Channel and the RRI Channel shall be time  
 6 multiplexed on the same Walsh channel as shown in Figure 9.2.1.3.1-2. The Pilot Channel  
 7 and the RRI Channel shall be transmitted at the same power.

8 9.2.1.3.3.2 Reverse Rate Indicator Channel

9 The RRI Channel is used by the access terminal to indicate the data rate at which the Data  
 10 Channel is transmitted. The data rate is represented by a three-bit RRI symbol at the rate  
 11 of one 3-bit symbol per 16-slot physical layer packet. Each RRI symbol shall be encoded  
 12 into a 7-bit codeword by a simplex encoder as specified in Table 9.2.1.3.3.2-1. Then, each  
 13 codeword shall be repeated 37 times and the last 3 symbols shall be disregarded (i.e.,  
 14 punctured), as shown in Figure 9.2.1.3.1-2. The resulting 256 binary symbols per physical  
 15 layer packet shall be time-division multiplexed with the Pilot Channel symbols and span the  
 16 same time interval as the corresponding physical layer packet. The time-division-  
 17 multiplexed Pilot and RRI Channel sequence shall be spread with the 16-chip Walsh  
 18 function  $W_0^{16}$  producing 256 RRI chips per slot. The RRI chips shall be time-division  
 19 multiplexed into the first 256 chips of every slot as shown in Figure 9.2.1.3.1-4. When no  
 20 physical layer packet is transmitted on the Reverse Traffic Channel, the access terminal  
 21 shall transmit the zero data rate RRI codeword on the RRI Channel, as specified in Table  
 22 9.2.1.3.3.2-1. The Pilot Channel and the RRI Channel shall be transmitted on the I  
 23 channel.

24 **Table 9.2.1.3.3.2-1. RRI Symbol and Simplex Encoder Assignments**

Data Rate (kbps)	RRI Symbol	RRI Codeword
0	000	0000000
9.6	001	1010101
19.2	010	0110011
38.4	011	1100110
76.8	100	0001111
153.6	101	1011010
Reserved	110	0111100
Reserved	111	1101001

25

26 9.2.1.3.3.3 Data Rate Control Channel

27 The DRC Channel is used by the access terminal to indicate to the access network the  
 28 selected serving sector and the requested data rate on the Forward Traffic Channel. The

1 requested Forward Traffic Channel data rate is mapped into a four-bit DRC value as  
2 specified by the Forward Traffic Channel MAC Protocol. An 8-ary Walsh function  
3 corresponding to the selected serving sector is used to spread the DRC Channel  
4 transmission. The cover mapping is defined by the public data DRCCover from the Forward  
5 Traffic Channel MAC Protocol.

6 The DRC values shall be transmitted at a data rate of  $600/\text{DRCLength}$  DRC values per  
7 second, where DRCLength is public data from the Forward Traffic Channel MAC Protocol.  
8 When DRCLength is greater than one, the DRC value and DRCCover inputs in Figure  
9 9.2.1.3.1-2 are repeated for DRCLength consecutive slots as specified in the Forward Traffic  
10 Channel MAC Protocol.

11 The DRC values shall be block encoded to yield 8-bit bi-orthogonal codewords, as specified  
12 in Table 9.2.1.3.3.3-1. Each DRC codeword shall be transmitted twice per slot. Each bit of a  
13 repeated codeword shall be spread by an 8-ary Walsh function  $W_i^8$  as defined in Table  
14 9.2.1.3.3.3-2, where i equals DRCCover. Each Walsh chip of the 8-ary Walsh function shall  
15 be further spread by the Walsh function  $W_8^{16}$ . Each DRC value shall be transmitted over  
16 DRCLength slots when the DRC Channel is continuously transmitted.

17 The access terminal may support gated DRC transmissions. For an access terminal that  
18 supports gated DRC transmissions, it shall gate its DRC transmissions if DRCGating equals  
19 1, where DRCGating is public data from the Forward Traffic Channel MAC Protocol. When  
20 the DRC transmissions are gated, each DRC symbol shall be transmitted over only one of  
21 every DRCLength slots as specified in the Forward Traffic Channel MAC Protocol. Slots  
22 where the DRC Channel is not gated off are called active slots.

23 The DRC Channel shall be transmitted on the Q Channel as shown in Figure 9.2.1.3.1-3.

24 The timing of the Forward Traffic Channel transmission corresponding to a DRC symbol  
25 shall be as specified by the Forward Traffic Channel MAC Protocol. The transmission of  
26 DRC symbols shall start at the mid-slot point. The timing for the Default Forward Traffic  
27 Channel MAC Protocol is shown in Figure 9.2.1.3.3.3-1 and Figure 9.2.1.3.3.3-2.

1

**Table 9.2.1.3.3.3-1. DRC Bi-Orthogonal Encoding<sup>43</sup>**

DRC Value	Codeword
0x0	00000000
0x1	11111111
0x2	01010101
0x3	10101010
0x4	00110011
0x5	11001100
0x6	01100110
0x7	10011001
0x8	00001111
0x9	11110000
0xA	01011010
0xB	10100101
0xC	00111100
0xD	11000011
0xE	01101001
0xF	10010110

2

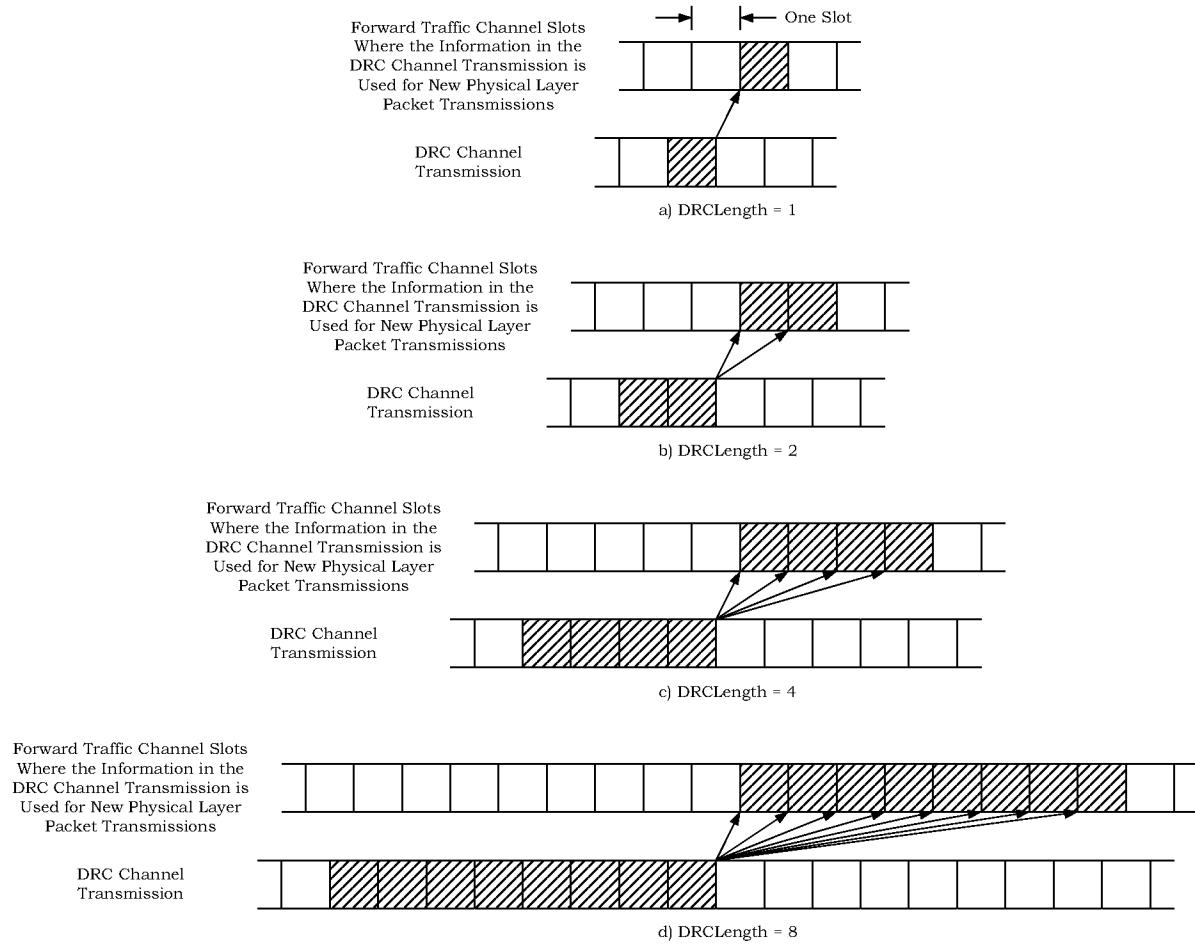
3

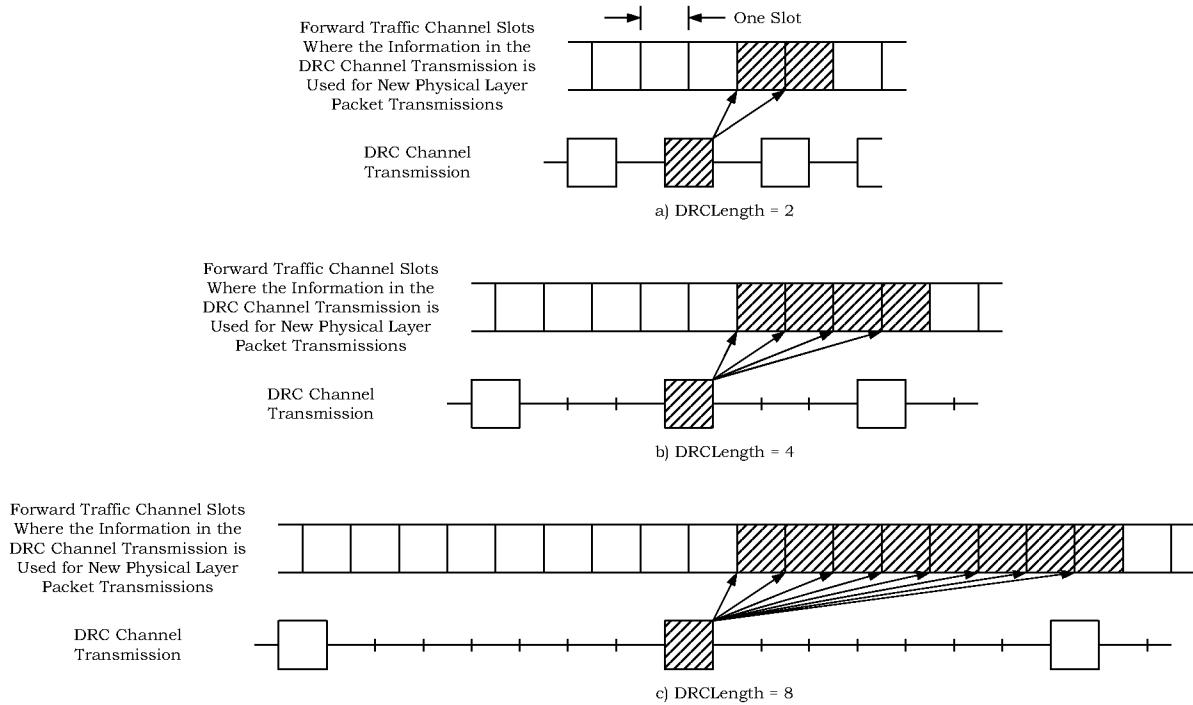
**Table 9.2.1.3.3.3-2. 8-ary Walsh Functions**

$W_0^8$	0000 0000
$W_1^8$	0101 0101
$W_2^8$	0011 0011
$W_3^8$	0110 0110
$W_4^8$	0000 1111
$W_5^8$	0101 1010
$W_6^8$	0011 1100
$W_7^8$	0110 1001

4

<sup>43</sup> The correspondence between data rates and DRC values is defined in Forward Traffic Channel MAC protocol (see Table 8.4.5.5.1.1-1).

**Figure 9.2.1.3.3.3-1. DRC Timing for Nongated Transmission**



**Figure 9.2.1.3.3-2. DRC Timing for Gated Transmission**

### 9.2.1.3.3.4 ACK Channel

The ACK Channel is used by the access terminal to inform the access network whether a physical layer packet transmitted on the Forward Traffic Channel has been received successfully or not. The access terminal shall transmit an ACK Channel bit in response to every Forward Traffic Channel slot that is associated with a detected preamble directed to the access terminal. The access terminal shall transmit at most one redundant positive ACK in response to a Forward Traffic Channel slot that is detected as a continuation of the physical layer packet that has been successfully received. Otherwise, the ACK Channel shall be gated off.

The ACK Channel shall be BPSK modulated. A '0' bit (ACK) shall be transmitted on the ACK Channel if a Forward Traffic Channel physical layer packet has been successfully received; otherwise, a '1' bit (NAK) shall be transmitted. A Forward Traffic Channel physical layer packet is considered successfully received if the FCS checks. For a Forward Traffic Channel physical layer packet transmitted in slot n on the Forward Channel, the corresponding ACK Channel bit shall be transmitted in slot n + 3 on the Reverse Channel (see Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6). The ACK Channel transmission shall be transmitted in the first half of the slot and shall last for 1024 PN chips as shown in Figure 9.2.1.3.1-5 and Figure 9.2.1.3.1-6. The ACK Channel shall use the Walsh channel identified by the Walsh function  $W_4^8$  and shall be transmitted on the I channel.

### 9.2.1.3.3.5 Data Channel

The Data Channel shall be transmitted at the data rates given in Table 9.2.1.3.1.1-1. Data transmissions shall only begin at slot FrameOffset within a frame. The FrameOffset

1 parameter is public data of the Reverse Traffic Channel MAC Protocol. All data transmitted  
 2 on the Reverse Traffic Channel shall be encoded, block interleaved, sequence repeated, and  
 3 orthogonally spread by Walsh function  $W_2^4$ .

4 **9.2.1.3.4 Encoding**

5 **9.2.1.3.4.1 Reverse Link Encoder Structure and Parameters**

6 The Reverse Traffic Channel and Access Channel physical layer packets shall be encoded  
 7 with code rates of 1/2 or 1/4, depending on the data rate. First, the encoder shall discard  
 8 the six bits of the TAIL field in the physical layer packet inputs (i.e., it shall discard the last  
 9 six bits in the input physical layer packets). Then, it shall encode the remaining bits with a  
 10 turbo encoder, as specified in 9.2.1.3.4.2. The turbo encoder will add an internally  
 11 generated tail.

12 The encoder parameters shall be as specified in Table 9.2.1.3.4.1-1.

13 **Table 9.2.1.3.4.1-1. Parameters for the Reverse Link Encoder**

<b>Data Rate (kbps)</b>	<b>9.6</b>	<b>19.2</b>	<b>38.4</b>	<b>76.8</b>	<b>153.6</b>
Reverse Rate Index	1	2	3	4	5
Code Rate	1/4	1/4	1/4	1/4	1/2
Bits per Physical Layer Packet	256	512	1,024	2,048	4,096
Number of Turbo Encoder Input Symbols	250	506	1,018	2,042	4,090
Turbo Encoder Code Rate	1/4	1/4	1/4	1/4	1/2
Encoder Output Block Length (Code Symbols)	1,024	2,048	4,096	8,192	8,192

14  
 15 **9.2.1.3.4.2 Turbo Encoding**

16 The turbo encoder encodes the input data and adds an output tail sequence. If the total  
 17 number of input bits is  $N_{\text{turbo}}$ , the turbo encoder generates  $N_{\text{turbo}}/R$  encoded data output  
 18 symbols followed by  $6/R$  tail output symbols, where  $R$  is the code rate of 1/2 or 1/4. The  
 19 turbo encoder employs two systematic, recursive, convolutional encoders connected in  
 20 parallel, with an interleaver, the turbo interleaver, preceding the second recursive  
 21 convolutional encoder.

1 The two recursive convolutional codes are called the constituent codes of the turbo code.  
 2 The outputs of the constituent encoders are punctured and repeated to achieve the  $(N_{\text{turbo}} + 6)/R$  output symbols.  
 3

4 9.2.1.3.4.2.1 Turbo Encoders

5 A common constituent code shall be used for the turbo codes of rate 1/2 and 1/4. The  
 6 transfer function for the constituent code shall be

$$7 \quad G(D) = \begin{bmatrix} 1 & \frac{n_0(D)}{d(D)} & \frac{n_1(D)}{d(D)} \end{bmatrix}$$

8 where  $d(D) = 1 + D^2 + D^3$ ,  $n_0(D) = 1 + D + D^3$ , and  $n_1(D) = 1 + D + D^2 + D^3$ .

9 The turbo encoder shall generate an output symbol sequence that is identical to the one  
 10 generated by the encoder shown in Figure 9.2.1.3.4.2.2-1. Initially, the states of the  
 11 constituent encoder registers in this figure are set to zero. Then, the constituent encoders  
 12 are clocked with the switches in the positions noted.

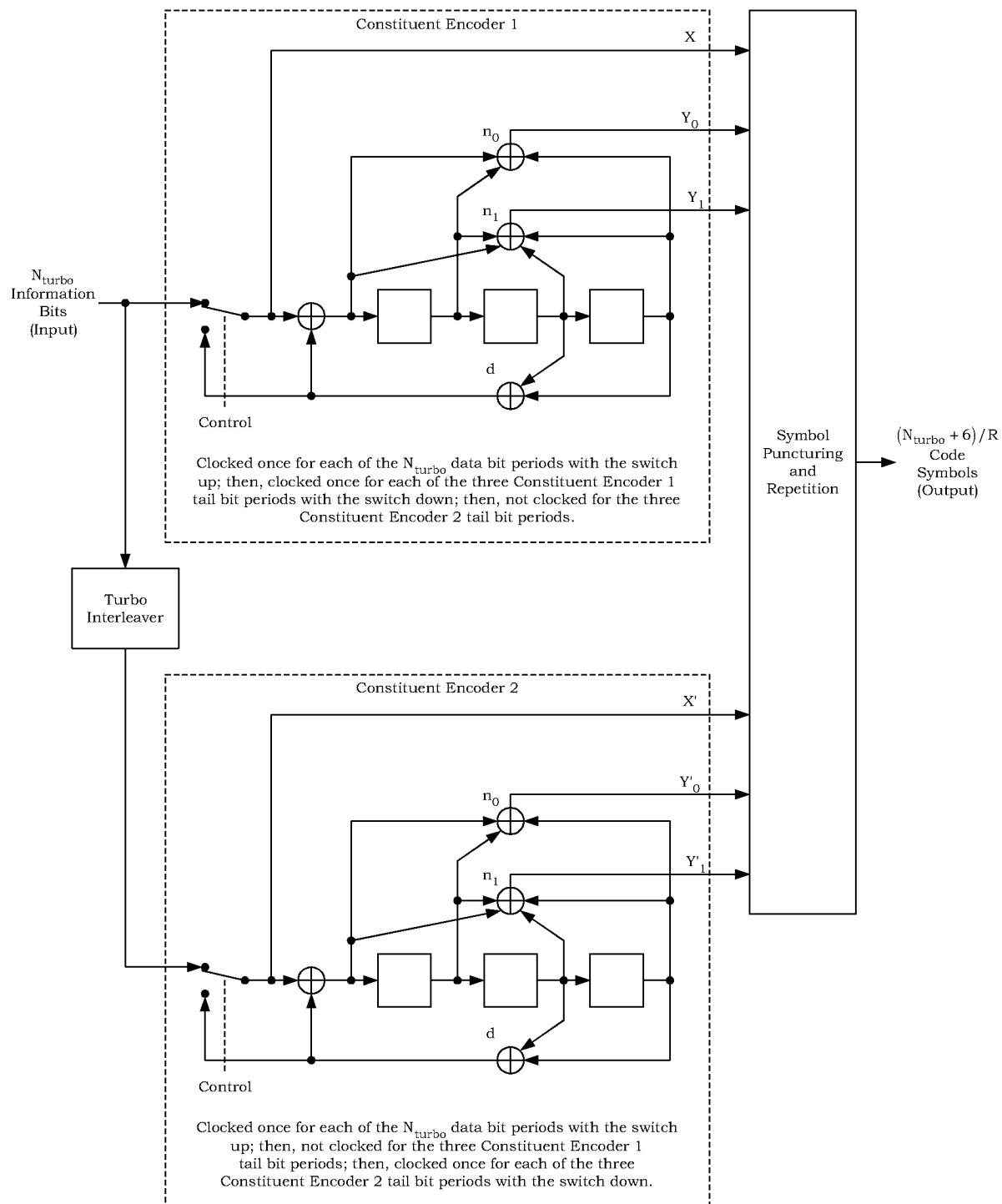
13 The encoded data output symbols are generated by clocking the constituent encoders  
 14  $N_{\text{turbo}}$  times with the switches in the up positions and puncturing the outputs as specified  
 15 in Table 9.2.1.3.4.2.2-1. Within a puncturing pattern, a '0' means that the symbol shall be  
 16 deleted and a '1' means that a symbol shall be passed. The constituent encoder outputs for  
 17 each bit period shall be output in the sequence  $X, Y_0, Y_1, X', Y'_0, Y'_1$  with the  $X$  output  
 18 first. Symbol repetition is not used in generating the encoded data output symbols.

19 9.2.1.3.4.2.2 Turbo Code Termination

20 The turbo encoder shall generate  $6/R$  tail output symbols following the encoded data output  
 21 symbols. This tail output symbol sequence shall be identical to the one generated by the  
 22 encoder shown in Figure 9.2.1.3.4.2.2-1. The tail output symbols are generated after the  
 23 constituent encoders have been clocked  $N_{\text{turbo}}$  times with the switches in the up position.

24 The first  $3/R$  tail output symbols are generated by clocking Constituent Encoder 1 three  
 25 times with its switch in the down position while Constituent Encoder 2 is not clocked and  
 26 puncturing and repeating the resulting constituent encoder output symbols. The last  $3/R$   
 27 tail output symbols are generated by clocking Constituent Encoder 2 three times with its  
 28 switch in the down position while Constituent Encoder 1 is not clocked and puncturing and  
 29 repeating the resulting constituent encoder output symbols. The constituent encoder  
 30 outputs for each bit period shall be output in the sequence  $X, Y_0, Y_1, X', Y'_0, Y'_1$  with the  $X$   
 31 output first.

32 The constituent encoder output symbol puncturing and symbol repetition shall be as  
 33 specified in Table 9.2.1.3.4.2.2-2. Within a puncturing pattern, a '0' means that the symbol  
 34 shall be deleted and a '1' means that a symbol shall be passed. For rate-1/2 turbo codes,  
 35 the tail output symbols for each of the first three tail bit periods shall be  $XY_0$ , and the tail  
 36 output symbols for each of the last three tail bit periods shall be  $X'Y'_0$ . For rate-1/4 turbo  
 37 codes, the tail output symbols for each of the first three tail bit periods shall be  $XXY_0Y_1$ ,  
 38 and the tail output symbols for each of the last three tail bit periods shall be  $XX'Y'_0Y_1$ .

**Figure 9.2.1.3.4.2.2-1. Turbo Encoder**

**Table 9.2.1.3.4.2.2-1. Puncturing Patterns for the Data Bit Periods**

<b>Output</b>	<b>Code Rate</b>	
	<b>1/2</b>	<b>1/4</b>
X	11	11
Y <sub>0</sub>	10	11
Y <sub>1</sub>	00	10
X'	00	00
Y' <sub>0</sub>	01	01
Y' <sub>1</sub>	00	11

Note: For each rate, the puncturing table shall be read first from top to bottom and then from left to right.

2

3

**Table 9.2.1.3.4.2.2-2. Puncturing Patterns for the Tail Bit Periods**

<b>Output</b>	<b>Code Rate</b>	
	<b>1/2</b>	<b>1/4</b>
X	111 000	111 000
Y <sub>0</sub>	111 000	111 000
Y <sub>1</sub>	000 000	111 000
X'	000 111	000 111
Y' <sub>0</sub>	000 111	000 111
Y' <sub>1</sub>	000 000	000 111

Note: For rate-1/2 turbo codes, the puncturing table shall be read first from top to bottom and then from left to right. For rate-1/4 turbo codes, the puncturing table shall be read first from top to bottom repeating X and X', and then from left to right.

4

5

### 9.2.1.3.4.2.3 Turbo Interleavers

6

7

The turbo interleaver, which is part of the turbo encoder, shall block interleave the turbo encoder input data that is fed to Constituent Encoder 2.

8

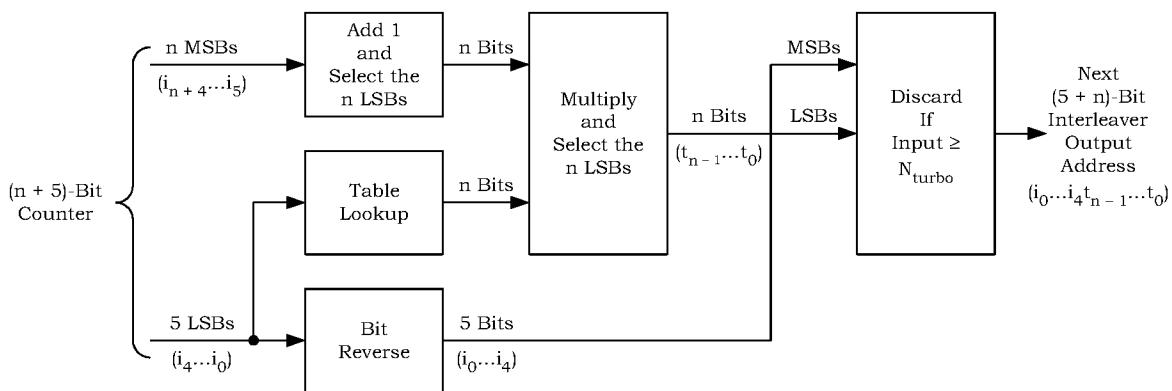
9

10

11

The turbo interleaver shall be functionally equivalent to an approach where the entire sequence of turbo interleaver input bits are written sequentially into an array at a sequence of addresses, and then the entire sequence is read out from a sequence of addresses that are defined by the procedure described below.

- Let the sequence of input addresses be from 0 to  $N_{\text{turbo}} - 1$ . Then, the sequence of interleaver output addresses shall be equivalent to those generated by the procedure illustrated in Figure 9.2.1.3.4.2.3-1 and described below.<sup>44</sup>
1. Determine the turbo interleaver parameter,  $n$ , where  $n$  is the smallest integer such that  $N_{\text{turbo}} \leq 2^{n+5}$ . Table 9.2.1.3.4.2.3-1 gives this parameter for the different physical layer packet sizes.
  2. Initialize an  $(n + 5)$ -bit counter to 0.
  3. Extract the  $n$  most significant bits (MSBs) from the counter and add one to form a new value. Then, discard all except the  $n$  least significant bits (LSBs) of this value.
  4. Obtain the  $n$ -bit output of the table lookup defined in Table 9.2.1.3.4.2.3-2 with a read address equal to the five LSBs of the counter. Note that this table depends on the value of  $n$ .
  5. Multiply the values obtained in Steps 3 and 4, and discard all except the  $n$  LSBs.
  6. Bit-reverse the five LSBs of the counter.
  7. Form a tentative output address that has its MSBs equal to the value obtained in Step 6 and its LSBs equal to the value obtained in Step 5.
  8. Accept the tentative output address as an output address if it is less than  $N_{\text{turbo}}$ ; otherwise, discard it.
  9. Increment the counter and repeat Steps 3 through 8 until all  $N_{\text{turbo}}$  interleaver output addresses are obtained.



**Figure 9.2.1.3.4.2.3-1. Turbo Interleaver Output Address Calculation Procedure**

<sup>44</sup> This procedure is equivalent to one where the counter values are written into a  $2^5$ -row by  $2^n$ -column array by rows, the rows are shuffled according to a bit-reversal rule, the elements within each row are permuted according to a row-specific linear congruential sequence, and tentative output addresses are read out by column. The linear congruential sequence rule is  $x(i + 1) = (x(i) + c) \bmod 2^n$ , where  $x(0) = c$  and  $c$  is a row-specific value from a table lookup.

1

**Table 9.2.1.3.4.2.3-1. Turbo Interleaver Parameter**

<b>Physical Layer Packet Size</b>	<b>Turbo Interleaver Block Size <math>N_{turbo}</math></b>	<b>Turbo Interleaver Parameter <math>n</math></b>
256	250	3
512	506	4
1,024	1,018	5
2,048	2,042	6
4,096	4,090	7

2

**Table 9.2.1.3.4.2.3-2. Turbo Interleaver Lookup Table Definition**

<b>Table Index</b>	<b>n = 3 Entries</b>	<b>n = 4 Entries</b>	<b>n = 5 Entries</b>	<b>n = 6 Entries</b>	<b>n = 7 Entries</b>
0	1	5	27	3	15
1	1	15	3	27	127
2	3	5	1	15	89
3	5	15	15	13	1
4	1	1	13	29	31
5	5	9	17	5	15
6	1	9	23	1	61
7	5	15	13	31	47
8	3	13	9	3	127
9	5	15	3	9	17
10	3	7	15	15	119
11	5	11	3	31	15
12	3	15	13	17	57
13	5	3	1	5	123
14	5	15	13	39	95
15	1	5	29	1	5
16	3	13	21	19	85
17	5	15	19	27	17
18	3	9	1	15	55
19	5	3	3	13	57
20	3	1	29	45	15
21	5	3	17	5	41
22	5	15	25	33	93
23	5	1	29	15	87
24	1	13	9	13	63
25	5	1	13	9	15
26	1	9	23	15	13
27	5	15	13	31	15
28	3	11	13	17	81
29	5	3	1	5	57
30	5	15	13	15	31
31	3	5	13	33	69

1    9.2.1.3.5 Channel Interleaving

2    The sequence of binary symbols at the output of the encoder shall be interleaved with a bit-  
3    reversal channel interleaver.

4    The bit-reversal channel interleaver shall be functionally equivalent to an approach where  
5    the entire sequence of symbols to be interleaved is written into a linear sequential array  
6    with addresses from 0 to  $2^L - 1$  and they are read out from a sequence of addresses based  
7    on the procedure described below.

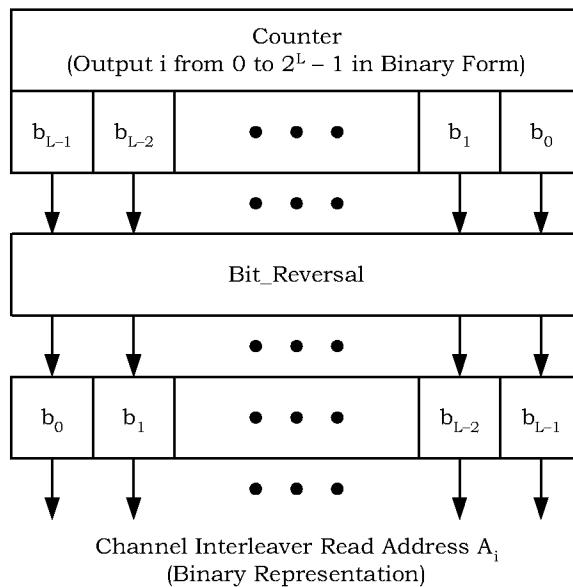
- 8    • The sequence of array addresses from which the interleaved symbols are read out is  
9    generated by a bit-reversal address generator.
- 10   • The  $i^{th}$  interleaved symbol is read out from the array element at address  $A_i$  that  
11   satisfies:

12                      
$$A_i = \text{Bit\_Reversal}(i, L)$$

13   where  $i = 0$  to  $2^L - 1$  and  $\text{Bit\_Reversal}(y, L)$  indicates the bit-reversed  $L$ -bit value of  $y$   
14   such that if  $i$  is expressed in the binary form of  $i = b_{L-1}b_{L-2}\dots b_1b_0$ , where  $b_k = 0$  or  $1$ ,  
15    $b_0$  is the LSB and  $b_L$  is the MSB,  $A_i = b_0b_1\dots b_{L-2}b_{L-1}$ .

- 16   • The bit-reversal interleaving process is completed when all of the symbols in the entire  
17   linear array are read out.

18   Figure 9.2.1.3.5-1 illustrates the procedure for generating the channel interleaver output  
19   address.



20                      **Figure 9.2.1.3.5-1. Channel Interleaver Address Generation**

22   9.2.1.3.6 Sequence Repetition

23   If the data rate is lower than 76.8 kbps, the sequence of interleaved code symbols shall be  
24   repeated before being modulated. The number of repeats varies for each data rate and shall

1 be as specified in Table 9.2.1.3.1.1-1. The repetition shall be functionally equivalent to  
 2 sequentially reading out all the symbols from the interleaver memory as many times as  
 3 necessary to achieve the fixed 307.2-ksps modulation symbol rate.

4 **9.2.1.3.7 Orthogonal Covers**

5 The Pilot Channel, consisting of the time-division-multiplexed Pilot and RRI Channels, the  
 6 DRC Channel, the ACK Channel, and the Data Channel shall be spread with Walsh  
 7 functions, also called Walsh covers, at a fixed chip rate of 1.2288 Mcps. Walsh function  
 8 time alignment shall be such that the first Walsh chip begins at a slot boundary referenced  
 9 to the access terminal transmission time.

10 The Walsh cover assignments are shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-2. The  
 11 Pilot Channel shall be covered by the 16-chip Walsh function number 0 ( $W_0^{16} =$   
 12  $+ + + + + + + + + + + + + + + +$ ). The DRC Channel shall be covered by the 16-chip Walsh  
 13 function number 8 ( $W_8^{16} = + + + + + + + + - - - - - - - -$ ). The ACK Channel shall be covered  
 14 by the 8-chip Walsh function number 4 ( $W_4^8 = + + + + - - - -$ ). The Data Channel shall be  
 15 covered by the 4-chip Walsh function number 2 ( $W_2^4 = + + - -$ ).

16 **9.2.1.3.8 Quadrature Spreading**

17 Following the orthogonal spreading, the ACK, DRC, and Data Channel chip sequences shall  
 18 be scaled by a factor that gives the gain of each of these channels relative to that of the Pilot  
 19 Channel. The relative gain values for the ACK and DRC Channels are specified by the  
 20 parameters AckChannelGain and DRCChannelGain which are public data of the Forward  
 21 Traffic Channel MAC Protocol. For the Reverse Traffic Channel, the relative gain of the Data  
 22 Channel is specified by parameters that are public data of the Reverse Traffic Channel MAC  
 23 Protocol as described in 9.2.1.2.4.1. For the Access Channel, the relative gain of the Data  
 24 Channel is specified by parameters that are public data of the Access Channel MAC  
 25 Protocol as described in 9.2.1.2.4.1.

26 After the scaling, the Pilot and scaled ACK, DRC, and Data Channel sequences are  
 27 combined to form resultant I-Channel and Q-Channel sequences, and these sequences are  
 28 quadrature spread as shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3. The quadrature  
 29 spreading shall occur at the chip rate of 1.2288 Mcps, and it shall be used for the Reverse  
 30 Traffic Channel and the Access Channel. The Pilot and scaled ACK Channel sequences shall  
 31 be added to form the resultant I-Channel sequence, and the scaled DRC and Data Channel  
 32 sequences shall be added to form the resultant Q-Channel sequence. The quadrature  
 33 spreading operation shall be equivalent to a complex multiply operation of the resultant I-  
 34 Channel and resultant Q-Channel sequences by the  $PN_I$  and  $PN_Q$  PN sequences, as shown  
 35 in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3.

36 The I and Q PN sequences,  $PN_I$  and  $PN_Q$ , shall be obtained from the long-code PN  
 37 sequences,  $U_I$  and  $U_Q$ , and the access terminal common short PN sequences,  $P_I$  and  $P_Q$ .  
 38 The binary long-code PN sequence and short PN sequence values of '0' and '1' shall be  
 39 mapped into values of +1 and -1, respectively.

1 The bipolar  $PN_I$  sequence values shall be equivalent to those obtained by multiplying the  
 2 bipolar  $P_I$  values by the bipolar  $U_I$  values.

3 The bipolar  $PN_Q$  sequence values shall be equivalent to those obtained with the following  
 4 procedure:

- 5 1. Multiply the bipolar  $P_Q$  values by the bipolar  $U_Q$  values.
- 6 2. Decimate the sequence of values obtained in Step 1 by a factor of two. That is, the  
 7 decimator provides an output that is constant for two consecutive chips by deleting  
 8 every other input value and repeating the previous input value in place of the  
 9 deleted value. The retained values shall align with the first chip of a slot.
- 10 3. Multiply pairs of decimator output symbols by the Walsh cover sequence (+ -). That  
 11 is, pass the first value of every pair unchanged and multiply the second value of  
 12 every pair by -1.
- 13 4. Multiply the sequence obtained in Step 3 by the bipolar  $PN_I$  sequence.

14 9.2.1.3.8.1 Access Terminal Common Short-Code PN Sequences

15 The access terminal common short-code PN sequences shall be the zero-offset I and Q PN  
 16 sequences with a period of  $2^{15}$  chips, and they shall be based on the following  
 17 characteristic polynomials, respectively:

18  $P_I(x) = x^{15} + x^{13} + x^9 + x^8 + x^7 + x^5 + 1$

19 (for the in-phase (I) sequence)

20 and

21  $P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$

22 (for the quadrature-phase (Q) sequence).

23 The maximum length linear feedback shift-register sequences  $\{I(n)\}$  and  $\{Q(n)\}$  based on the  
 24 above are of length  $2^{15} - 1$  and can be generated by the following linear recursions:

25  $I(n) = I(n - 15) \oplus I(n - 10) \oplus I(n - 8) \oplus I(n - 7) \oplus I(n - 6) \oplus I(n - 2)$

26 (based on  $P_I(x)$  as the characteristic polynomial)

27 and

28  $Q(n) = Q(n - 15) \oplus Q(n - 12) \oplus Q(n - 11) \oplus Q(n - 10) \oplus Q(n - 9) \oplus$   
 29  $Q(n - 5) \oplus Q(n - 4) \oplus Q(n - 3)$

30 (based on  $P_Q(x)$  as the characteristic polynomial),

31 where  $I(n)$  and  $Q(n)$  are binary valued ('0' and '1') and the additions are modulo-2. In order  
 32 to obtain the I and Q common short-code PN sequences (of period  $2^{15}$ ), a '0' is inserted in  
 33 the  $\{I(n)\}$  and  $\{Q(n)\}$  sequences after 14 consecutive '0' outputs (this occurs only once in each  
 34 period). Therefore, the short-code PN sequences have one run of 15 consecutive '0' outputs  
 35 instead 14. The initial state of the access terminal common short-code PN sequences, both I

1 and Q, shall be that state in which the output of the short-code PN sequence generator is  
 2 the '1' following the 15 consecutive '0' outputs.

3 The chip rate for the access terminal common short-code PN sequence shall be 1.2288  
 4 Mcps. The short-code PN sequence period is  $32768/1228800 = 26.666\dots$  ms, and exactly 75  
 5 PN sequences repetitions occur every 2 seconds.

6 The access terminal shall align the I and Q short-code PN sequences such that the first chip  
 7 on every even-second mark as referenced to the transmit time reference (see 9.2.1.5) is the  
 8 '1' after the 15 consecutive '0's (see Figure 1.13-1).

#### 9 9.2.1.3.8.2 Long Codes

10 The in-phase and quadrature-phase long codes,  $U_I$  and  $U_Q$ , shall be generated from a  
 11 sequence, called the long-code generating sequence, by using two different masks. The  
 12 long-code generating sequence shall satisfy the linear recursion specified by the following  
 13 characteristic polynomial:

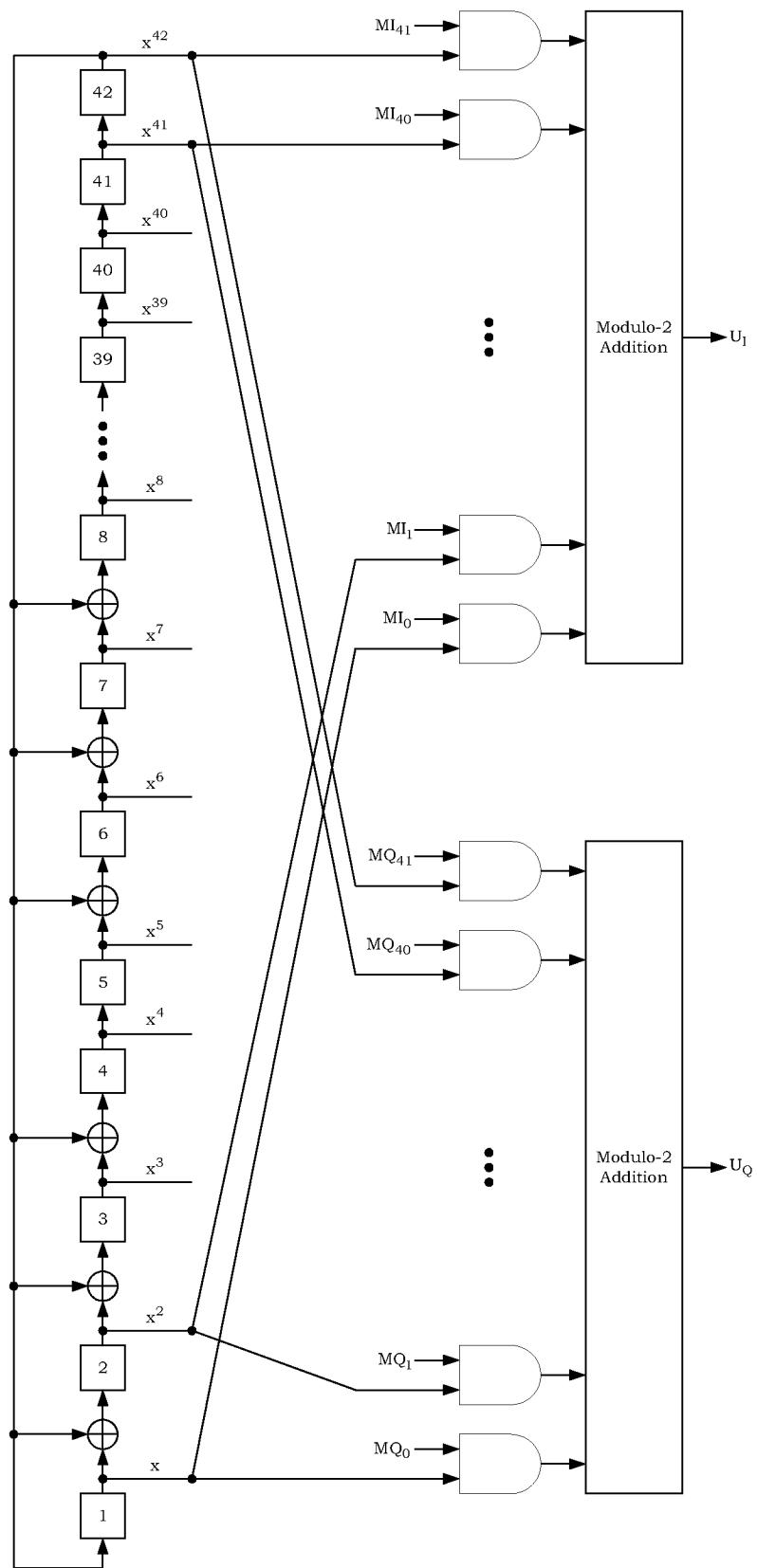
$$14 \quad p(x) = x^{42} + x^{35} + x^{33} + x^{31} + x^{27} + x^{26} + x^{25} + x^{22} + x^{21} + x^{19} + \\ 15 \quad x^{18} + x^{17} + x^{16} + x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1.$$

16 The long codes,  $U_I$  and  $U_Q$ , shall be generated by a modulo-2 inner product of the 42-bit  
 17 state vector of the sequence generator and two 42-bit masks, MI and MQ, respectively, as  
 18 shown in Figure 9.2.1.3.8.2-1. The masks MI and MQ vary depending on the channel on  
 19 which the access terminal is transmitting.

20 For transmission on the Access Channel, MI and MQ shall be set to  $MI_{ACMAC}$  and  
 21  $MQ_{ACMAC}$  (given as public data of the Access Channel MAC Protocol), respectively, and the  
 22 long-code sequences are referred to as the access long codes.

23 For transmission on the Reverse Traffic Channel, MI and MQ shall be set to  $MI_{RTCMAC}$  and  
 24  $MQ_{RTCMAC}$  (given as public data of the Reverse Traffic Channel MAC Protocol), respectively,  
 25 and the long-code sequences are referred to as the user long codes.

26 The long code generator shall be reloaded with the hexa-decimal value 0x24B91BFD3A8 at  
 27 the beginning of every period of the short codes. Thus, the long codes are periodic with a  
 28 period of  $2^{15}$  PN chips.



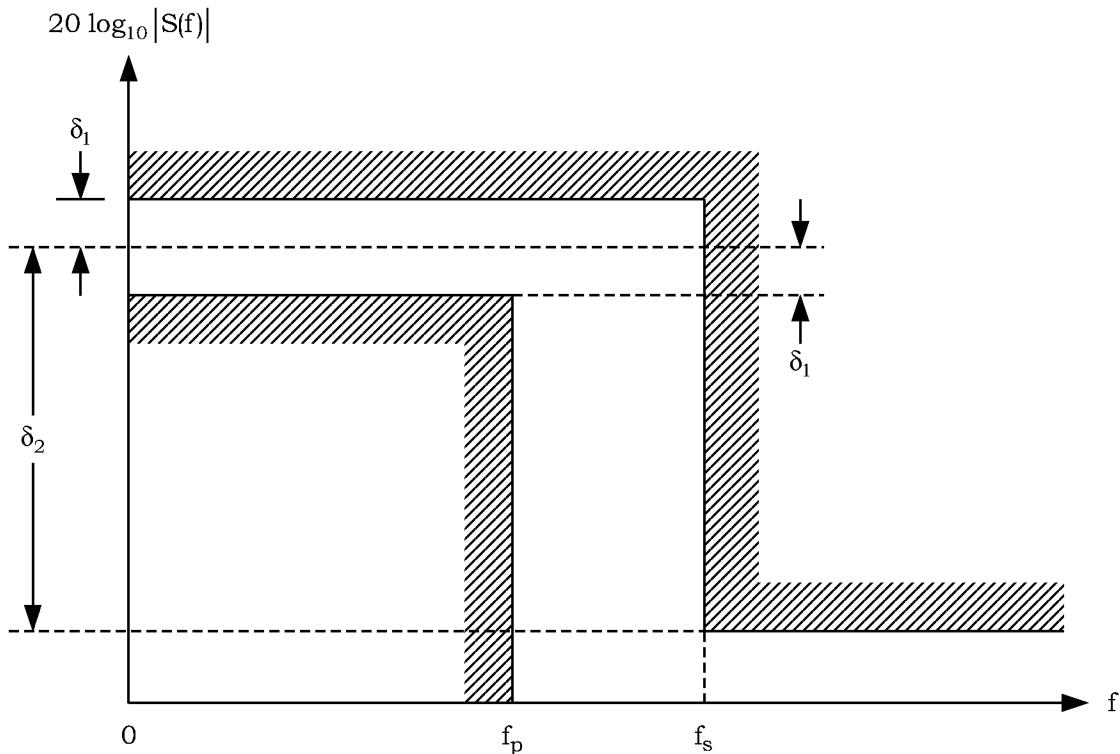
1

2

**Figure 9.2.1.3.8.2-1. Long-Code Generators**

### 9.2.1.3.8.3 Baseband Filtering

Following the quadrature spreading operation, the I' and Q' impulses are applied to the inputs of the I and Q baseband filters as shown in Figure 9.2.1.3.1-1 and Figure 9.2.1.3.1-3. The baseband filters shall have a frequency response  $S(f)$  that satisfies the limits given in Figure 9.2.1.3.8-2. Specifically, the normalized frequency response of the filter shall be contained within  $\pm\delta_1$  in the passband  $0 \leq f \leq f_p$  and shall be less than or equal to  $-\delta_2$  in the stopband  $f \geq f_s$ . The numerical values for the parameters are  $\delta_1 = 1.5$  dB,  $\delta_2 = 40$  dB,  $f_p = 590$  kHz, and  $f_s = 740$  kHz.



**Figure 9.2.1.3.8-2. Baseband Filter Frequency Response Limits**

The impulse response of the baseband filter,  $s(t)$ , should satisfy the following equation:

$$\text{Mean Squared Error} = \sum_{k=0}^{\infty} [\alpha s(kT_s - \tau) - h(k)]^2 \leq 0.03,$$

where the constants  $\alpha$  and  $\tau$  are used to minimize the mean squared error. The constant  $T_s$  is equal to 203.451... ns, which equals one quarter of a PN chip. The values of the coefficients  $h(k)$ , for  $k < 48$ , are given in Table 9.2.1.3.8-1;  $h(k) = 0$  for  $k \geq 48$ . Note that  $h(k)$  equals  $h(47 - k)$ .

**Table 9.2.1.3.8-1. Baseband Filter Coefficients**

<b>k</b>	<b>h(k)</b>
0, 47	-0.025288315
1, 46	-0.034167931
2, 45	-0.035752323
3, 44	-0.016733702
4, 43	0.021602514
5, 42	0.064938487
6, 41	0.091002137
7, 40	0.081894974
8, 39	0.037071157
9, 38	-0.021998074
10, 37	-0.060716277
11, 36	-0.051178658
12, 35	0.007874526
13, 34	0.084368728
14, 33	0.126869306
15, 32	0.094528345
16, 31	-0.012839661
17, 30	-0.143477028
18, 29	-0.211829088
19, 28	-0.140513128
20, 27	0.094601918
21, 26	0.441387140
22, 25	0.785875640
23, 24	1.0

2

## 3      9.2.1.4 Closed-Loop Power-Control Operation

4      Once the connection is established, the access network continuously transmits '0' (up) or '1'  
 5      (down) RPC bits to the access terminal, based on measurements of the reverse link signal  
 6      quality. If the received quality is above the target threshold, a '1' bit is transmitted. If the  
 7      received quality is below the target threshold, a '0' bit is transmitted. The access terminal  
 8      shall adjust its output power by a discrete amount in the direction indicated by the RPC bit  
 9      after the RPC bit is received as specified in 9.2.1.2.4.2 and 9.2.1.2.5.2. The RPC bit is

1 considered received after the 64-chip MAC burst following the second pilot burst of a slot is  
2 received as shown in Figure 9.3.1.3.1-2.

3 The SofterHandoff public data of the Route Update Protocol indicates whether or not two  
4 different sectors are transmitting the same RPC bit. In each slot containing power control  
5 bits, the access terminal should provide diversity combining of the identical RPC Channels  
6 and shall obtain at most one power control bit from each set of identical RPC Channels. The  
7 access terminal shall increase its output power if all the resulting RPC bits are '0' ("up"). If  
8 any resulting RPC bit is '1' ("down"), the access terminal shall decrease its output power as  
9 specified in 9.2.1.2.4.2.

10 **9.2.1.5 Synchronization and Timing**

11 The nominal relationship between the access terminal and access network transmit and  
12 receive time references shall be as shown in Figure 1.13-1. The access terminal shall  
13 establish a time reference that is used to derive timing for the transmitted chips, symbols,  
14 slots, frames, and system timing. The access terminal initial time reference shall be  
15 established from the acquired Pilot Channel and from the Sync message transmitted on the  
16 Control Channel. Under steady-state conditions, the access terminal time reference shall be  
17 within  $\pm 1 \mu s$  of the time of occurrence, as measured at the access terminal antenna  
18 connector, of the earliest arriving multipath component being used for demodulation. If  
19 another multipath component belonging to the same Pilot Channel or to a different Pilot  
20 Channel becomes the earliest arriving multipath component to be used, the access terminal  
21 time reference shall track to the new component. If the difference between the access  
22 terminal time reference and the time of occurrence of the earliest arriving multipath  
23 component being used for demodulation, as measured at the access terminal antenna  
24 connector, is less than  $\pm 1 \mu s$ , the access terminal may directly track its time reference to  
25 the earliest arriving multipath component being used for demodulation.

26 If an access terminal time reference correction is needed, it shall be corrected no faster than  
27 203 ns (1/4 chip) in any 200-ms period and no slower than 305 ns (3/8 PN chip) per  
28 second.

29 The access terminal time reference shall be used as the transmit time reference of the  
30 Reverse Traffic Channel and the Access Channel.

31

**9.3 Access Network Requirements**

This section defines requirements specific to access network equipment and operation.

**9.3.1 Transmitter**

The transmitter shall reside in each sector of the access network. These requirements apply to the transmitter in each sector.

**9.3.1.1 Frequency Parameters****9.3.1.1.1 Channel Spacing and Designation****9.3.1.1.1.1 Band Class 0 (800-MHz Band)**

The Band Class 0 system designators for access network transmissions shall be as specified in Table 9.2.1.1.1.1-1. Access networks supporting Band Class 0 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.1-2 and as described in Table 9.2.1.1.1.1-3.

**9.3.1.1.1.2 Band Class 1 (1900-MHz Band)**

The Band Class 1 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.2-1. Access networks supporting Band Class 1 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.2-2 and as described in Table 9.2.1.1.1.2-3.

**9.3.1.1.1.3 Band Class 2 (TACS Band)**

The Band Class 2 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.3-1. Access networks supporting Band Class 2 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.3-3 and as described in Table 9.2.1.1.1.3-4.

**9.3.1.1.1.4 Band Class 3 (JTACS Band)**

The Band Class 3 system designators for access network transmissions shall be as specified in Table 9.2.1.1.1.4-1. Access networks supporting Band Class 3 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.4-2 and as described in Table 9.2.1.1.1.4-3.

**9.3.1.1.1.5 Band Class 4 (Korean PCS Band)**

The Band Class 4 block designators for access network transmissions shall be as specified in Table 9.2.1.1.1.5-1. Access networks supporting Band Class 4 shall support operations on CDMA Channels as calculated in Table 9.2.1.1.1.5-2 and as described in Table 9.2.1.1.1.5-3.

1    9.3.1.1.6 Band Class 5 (450-MHz Band)

2    The Band Class 5 block designators for access network transmissions shall be as specified  
3    in Table 9.2.1.1.6-1. Access networks supporting Band Class 5 shall support operations  
4    on CDMA Channels as calculated in Table 9.2.1.1.6-2 and as described in Table  
5    9.2.1.1.6-3.

6    9.3.1.1.7 Band Class 6 (2-GHz Band)

7    The Band Class 6 block designators for access network transmissions are not specified.  
8    Access networks supporting Band Class 6 shall support operations on CDMA Channels as  
9    calculated in Table 9.2.1.1.7-1 and as described in Table 9.2.1.1.7-2.

10   9.3.1.1.8 Band Class 7 (700-MHz Band)

11   The Band Class 7 block designators for access network transmissions shall be as specified  
12   in Table 9.2.1.1.8-1. Access networks supporting Band Class 7 shall support operations  
13   on CDMA Channels as calculated in Table 9.2.1.1.8-2 and as described in Table  
14   9.2.1.1.8-3.

15   9.3.1.1.9 Band Class 8 (1800-MHz Band)

16   The Band Class 8 block designators for access network transmissions are not specified.  
17   Access networks supporting Band Class 8 shall support operations on CDMA Channels as  
18   calculated in Table 9.2.1.1.9-1 and as described in Table 9.2.1.1.9-2.

19   9.3.1.1.10 Band Class 9 (900-MHz Band)

20   The Band Class 9 block designators for access network transmissions are not specified.  
21   Access networks supporting Band Class 9 shall support operations on CDMA Channels as  
22   calculated in Table 9.2.1.1.10-1 and as described in Table 9.2.1.1.10-2.

23   9.3.1.1.2 Frequency Tolerance

24   The average frequency difference between the actual sector transmit carrier frequency and  
25   the specified sector transmit frequency assignment shall be less than  $\pm 5 \times 10^{-8}$  of the  
26   frequency assignment ( $\pm 0.05$  ppm).

27   9.3.1.2 Power Output Characteristics

28   The access network shall meet the requirements in the current version of [4].

29   9.3.1.3 Modulation Characteristics

30   9.3.1.3.1 Forward Channel Structure

31   The Forward Channel shall have the overall structure shown in Figure 9.3.1.3.1-1. The  
32   Forward Channel shall consist of the following time-multiplexed channels: the Pilot  
33   Channel, the Forward Medium Access Control (MAC) Channel, and the Forward Traffic  
34   Channel or the Control Channel. The Traffic Channel carries user physical layer packets.

1 The Control Channel carries control messages, and it may also carry user traffic. Each  
2 channel is further decomposed into code-division-multiplexed quadrature Walsh channels.

3 The forward link shall consist of slots of length 2048 chips (1.66... ms). Groups of 16 slots  
4 shall be aligned to the PN rolls of the zero-offset PN sequences and shall align to system  
5 time on even-second ticks.

6 Within each slot, the Pilot, MAC, and Traffic or Control Channels shall be time-division  
7 multiplexed as shown in Figure 9.3.1.3.1-2 and shall be transmitted at the same power  
8 level.

9 The Pilot Channel shall consist of all-'0' symbols transmitted on the I channel with Walsh  
10 cover 0. Each slot shall be divided into two half slots, each of which contains a pilot burst.  
11 Each pilot burst shall have a duration of 96 chips and be centered at the midpoint of the  
12 half slot.<sup>45</sup>

13 The MAC Channel shall consist of two subchannels: the Reverse Power Control (RPC)  
14 Channel and the Reverse Activity (RA) Channel. The RA Channel transmits a reverse link  
15 activity bit (RAB) stream.

16 Each MAC Channel symbol shall be BPSK modulated on one of 64 64-ary Walsh codewords  
17 (covers). The MAC symbol Walsh covers shall be transmitted four times per slot in bursts of  
18 64 chips each. A burst shall be transmitted immediately preceding each of the pilot bursts  
19 in a slot, and a burst shall be transmitted immediately following each of the pilot bursts in  
20 a slot. The Walsh channel gains may vary the relative power.

21 The Forward Traffic Channel is a packet-based, variable-rate channel. The user physical  
22 layer packets for an access terminal shall be transmitted at a data rate that varies from  
23 38.4 kbps to 2.4576 Mbps.<sup>46</sup>

24 The Forward Traffic Channel and Control Channel data shall be encoded in blocks called  
25 physical layer packets. The output of the encoder shall be scrambled and then fed into a  
26 channel interleaver. The output of the channel interleaver shall be fed into a QPSK/8-  
27 PSK/16-QAM modulator. The modulated symbol sequences shall be repeated and  
28 punctured, as necessary. Then, the resulting sequences of modulation symbols shall be  
29 demultiplexed to form 16 pairs (in-phase and quadrature) of parallel streams. Each of the  
30 parallel streams shall be covered with a distinct 16-ary Walsh function at a chip rate to  
31 yield Walsh symbols at 76.8 ksps. The Walsh-coded symbols of all the streams shall be  
32 summed together to form a single in-phase stream and a single quadrature stream at a chip  
33 rate of 1.2288 Mcps. The resulting chips are time-division multiplexed with the preamble,

---

<sup>45</sup> The pilot is used by the access terminal for initial acquisition, phase recovery, timing recovery, and maximal-ratio combining. An additional function of the pilot is to provide the access terminal with a means of predicting the receive C/I for the purpose of access-terminal-directed forward data rate control (DRC) of the Data Channel transmission.

<sup>46</sup> The DRC symbol from the access terminal is based primarily on its estimate of the forward C/I for the duration of the next possible forward link packet transmission.

1 Pilot Channel, and MAC Channel chips to form the resultant sequence of chips for the  
2 quadrature spreading operation.

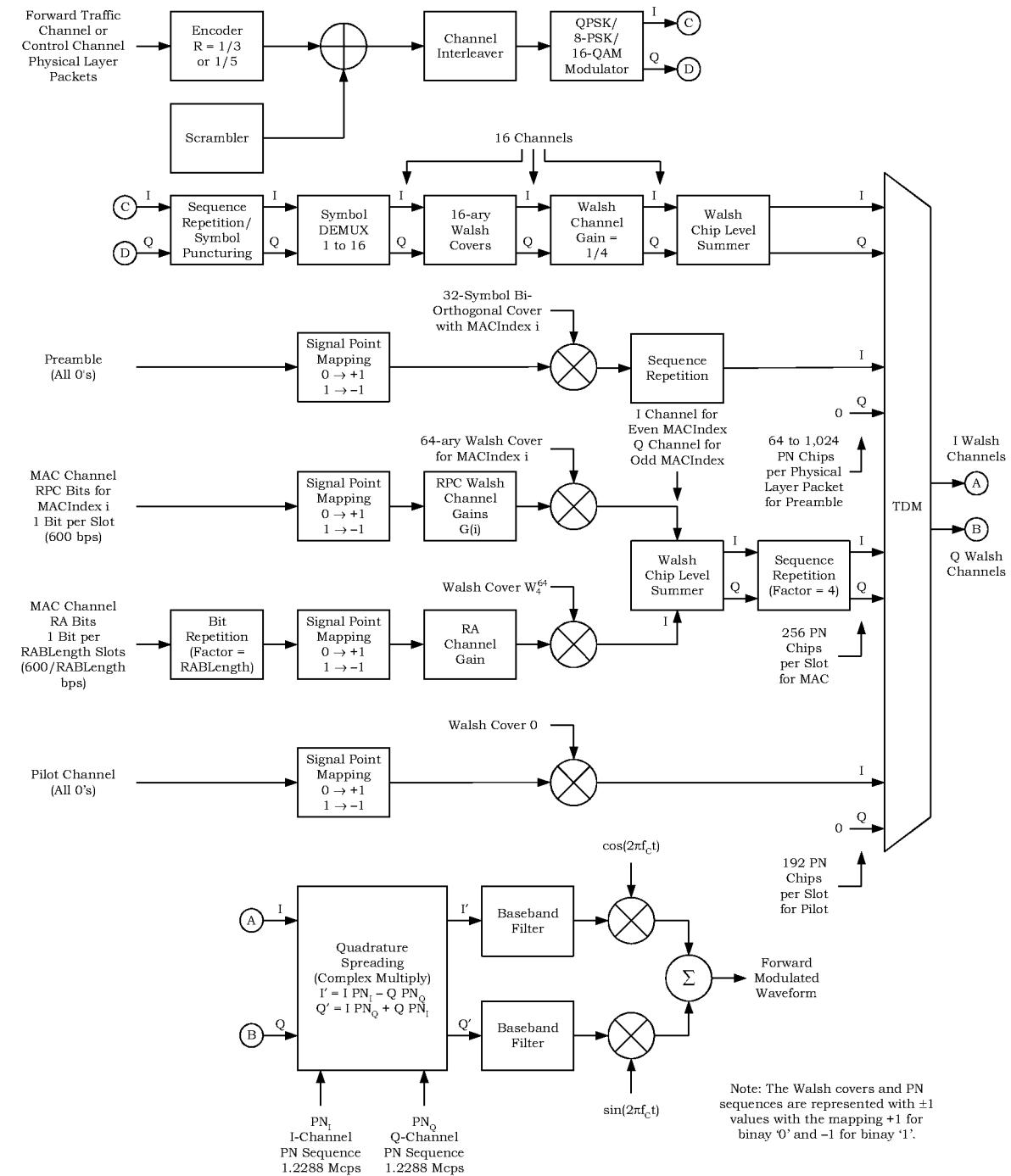
3 Forward Traffic Channel and Control Channel physical layer packets can be transmitted in  
4 1 to 16 slots (see Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2). When more than one slot is  
5 allocated, the transmit slots shall use a 4-slot interlacing. That is, the transmit slots of a  
6 physical layer packet shall be separated by three intervening slots, and slots of other  
7 physical layer packets shall be transmitted in the slots between those transmit slots. If a  
8 positive acknowledgement is received on the reverse link ACK Channel before all of the  
9 allocated slots have been transmitted, the remaining untransmitted slots shall not be  
10 transmitted and the next allocated slot may be used for the first slot of the next physical  
11 layer packet transmission.

12 Figure 9.3.1.3.1-3 and Figure 9.3.1.3.1-4 illustrate the multislot interlacing approach for a  
13 153.6-kbps Forward Traffic Channel with DRCLength of one slot. The 153.6-kbps Forward  
14 Traffic Channel physical layer packets use four slots, and these slots are transmitted with a  
15 three-slot interval between them, as shown in the figures. The slots from other physical  
16 layer packets are interlaced in the three intervening slots. Figure 9.3.1.3.1-3 shows the case  
17 of a normal physical layer packet termination. In this case, the access terminal transmits  
18 NAK responses on the ACK Channel after the first three slots of the physical layer packet  
19 are received indicating that it was unable to correctly receive the Forward Traffic Channel  
20 physical layer packet after only one, two, or three of the nominal four slots. An ACK or NAK  
21 is also transmitted after the last slot is received, as shown. Figure 9.3.1.3.1-4 shows the  
22 case where the Forward Traffic Channel physical layer packet transmission is terminated  
23 early. In this example, the access terminal transmits an ACK response on the ACK Channel  
24 after the third slot is received indicating that it has correctly received the physical layer  
25 packet. When the access network receives such an ACK response, it does not transmit the  
26 remaining slots of the physical layer packet. Instead, it may begin transmission of any  
27 subsequent physical layer packets.

28 When the access network has transmitted all the slots of a physical layer packet or has  
29 received a positive ACK response, the physical layer shall return a *ForwardTrafficCompleted*  
30 indication.

31 The Control Channel shall be transmitted at a data rate of 76.8 kbps or 38.4 kbps. The  
32 modulation characteristics for the Control Channel shall be the same as those of the  
33 Forward Traffic Channel transmitted at the corresponding rate.

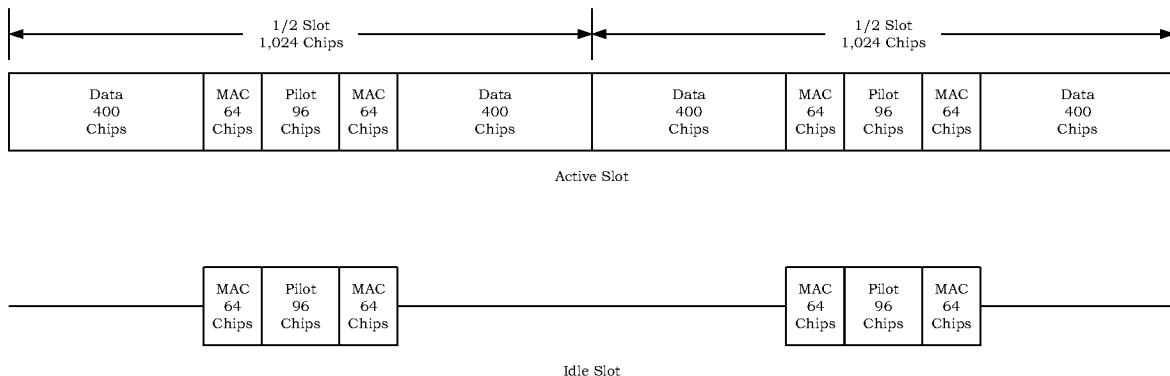
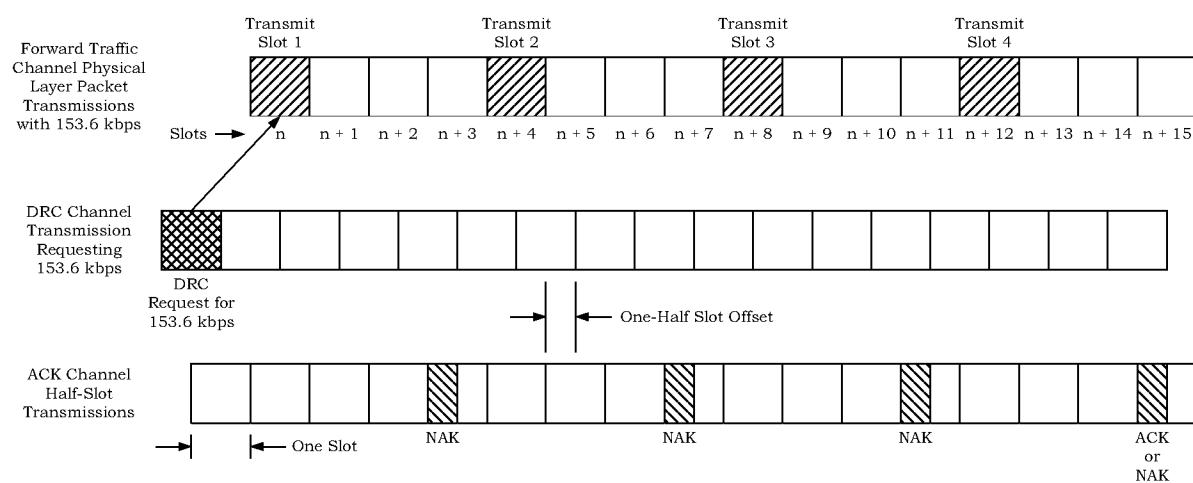
34 The Forward Traffic Channel and Control Channel data symbols shall fill the slot as shown  
35 in Figure 9.3.1.3.1-2. A slot during which no traffic or control data is transmitted is referred  
36 to as an idle slot. During an idle slot, the sector shall transmit the Pilot Channel and the  
37 MAC Channel, as described earlier.

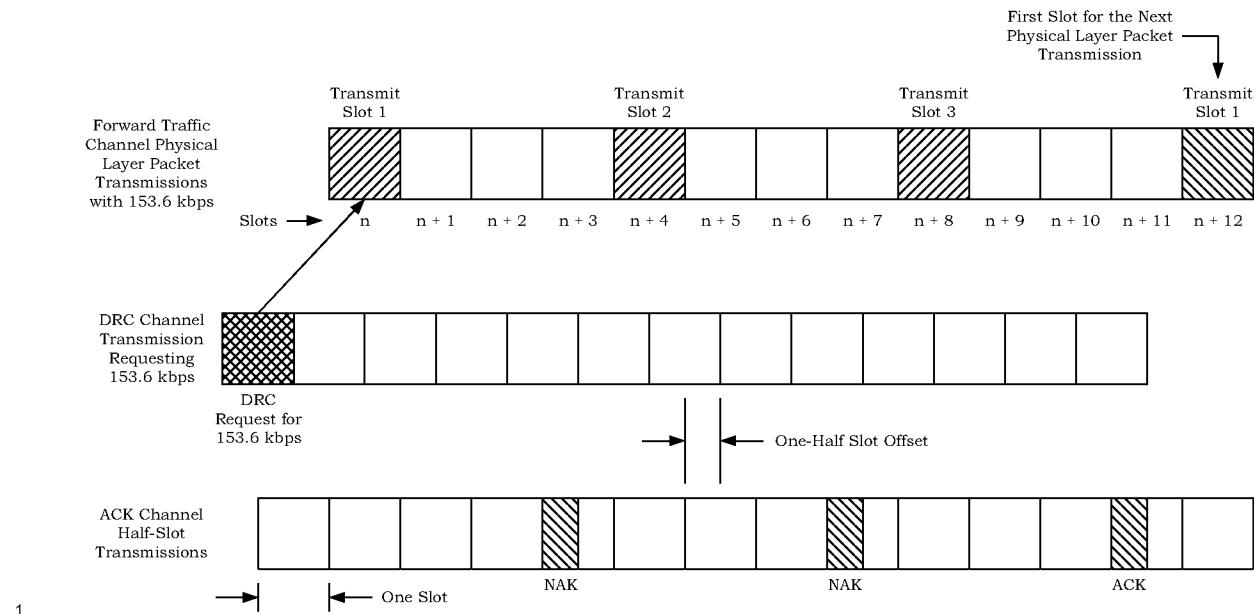


1

2

**Figure 9.3.1.3.1-1. Forward Channel Structure**

**Figure 9.3.1.3.1-2. Forward Link Slot Structure****Figure 9.3.1.3.1-3. Multislot Physical Layer Packet with Normal Termination**



**Figure 9.3.1.3.1-4. Multislot Physical Layer Packet with Early Termination**

### 9.3.1.3.1.1 Modulation Parameters

The modulation parameters for the Forward Traffic Channel and the Control Channel shall be as shown in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2. The Control Channel shall only use the 76.8 kbps and 38.4 kbps data rates.

1      **Table 9.3.1.3.1.1-1. Modulation Parameters for the Forward Traffic Channel and the**  
 2      **Control Channel (Part 1 of 2)**

<b>Data Rate (kbps)</b>	<b>Number of Values per Physical Layer Packet</b>				
	<b>Slots</b>	<b>Bits</b>	<b>Code Rate</b>	<b>Modulation Type</b>	<b>TDM Chips (Preamble, Pilot, MAC, Data)</b>
38.4	16	1,024	1/5	QPSK	1,024 3,072 4,096 24,576
76.8	8	1,024	1/5	QPSK	512 1,536 2,048 12,288
153.6	4	1,024	1/5	QPSK	256 768 1,024 6,144
307.2	2	1,024	1/5	QPSK	128 384 512 3,072
614.4	1	1,024	1/3	QPSK	64 192 256 1,536

3

**Table 9.3.1.3.1.1-2. Modulation Parameters for the Forward Traffic Channel and the Control Channel (Part 2 of 2)**

<b>Data Rate (kbps)</b>	<b>Number of Values per Physical Layer Packet</b>				
	<b>Slots</b>	<b>Bits</b>	<b>Code Rate</b>	<b>Modulation Type</b>	<b>TDM Chips (Preamble, Pilot, MAC, Data)</b>
307.2	4	2,048	1/3	QPSK	128 768 1,024 6,272
614.4	2	2,048	1/3	QPSK	64 384 512 3,136
1,228.8	1	2,048	1/3	QPSK	64 192 256 1,536
921.6	2	3,072	1/3	8-PSK	64 384 512 3,136
1,843.2	1	3,072	1/3	8-PSK	64 192 256 1,536
1,228.8	2	4,096	1/3	16-QAM	64 384 512 3,136
2,457.6	1	4,096	1/3	16-QAM	64 192 256 1,536

<sup>3</sup>

<sup>4</sup> The modulation parameters for the MAC Channel shall be as shown in Table 9.3.1.3.1.1-3.

**Table 9.3.1.3.1.1-3. Modulation Parameters for the MAC Channel**

<b>Parameter</b>	<b>RPC Channel</b>	<b>RA Channel</b>
Rate (bps)	600	600/RABLength
Bit Repetition Factor	1	RABLength
Modulation (Channel)	BPSK (I or Q)	BPSK (I)
Modulation Symbol Rate (sps)	2,400	2,400
Walsh Cover Length	64	64
Walsh Sequence Repetition Factor	4	4
PN Chips/Slot	256	256
PN Chips/Bit	256	256 × RABLength

2

## 3 9.3.1.3.1.2 Data Rates

4 The Forward Traffic Channel shall support variable-data-rate transmission from 38.4 kbps  
5 to 2.4576 Mbps, as shown in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2.

6 The data rate of the Control Channel shall be 76.8 kbps or 38.4 kbps.

## 7 9.3.1.3.2 Forward Link Channels

## 8 9.3.1.3.2.1 Pilot Channel

9 A Pilot Channel shall be transmitted at all times by the sector on each active Forward  
10 Channel. The Pilot Channel is an unmodulated signal that is used for synchronization and  
11 other functions by an access terminal operating within the coverage area of the sector. The  
12 Pilot Channel shall be transmitted at the full sector power.

## 13 9.3.1.3.2.1.1 Modulation

14 The Pilot Channel shall consist of all-'0' symbols transmitted on the I component only.

## 15 9.3.1.3.2.1.2 Orthogonal Spreading

16 The Pilot Channel shall be assigned Walsh cover 0.

## 17 9.3.1.3.2.1.3 Quadrature Spreading

18 See 9.3.1.3.4.

## 1    9.3.1.3.2.2 Forward MAC Channel

2    The Forward MAC Channel shall be composed of Walsh channels that are orthogonally  
 3    covered and BPSK modulated on a particular phase of the carrier (either in-phase or  
 4    quadrature phase). Each Walsh channel shall be identified by a MACIndex value that is  
 5    between 0 and 63 and defines a unique 64-ary Walsh cover and a unique modulation  
 6    phase. The Walsh functions assigned to the MACIndex values shall be as follows:

$$7 \quad W_{i/2}^{64} \text{ for } i = 0, 2, \dots, 62$$

$$W_{(i-1)/2+32}^{64} \text{ for } i = 1, 3, \dots, 63$$

8    where i is the MACIndex value. MAC Channels with even-numbered MACIndex values shall  
 9    be assigned to the in-phase (I) modulation phase, while those with odd-numbered  
 10   MACIndex values shall be assigned to the quadrature (Q) modulation phase. The MAC  
 11   symbol Walsh covers shall be transmitted four times per slot in bursts of length 64 chips  
 12   each. These bursts shall be transmitted immediately preceding and following the pilot  
 13   bursts of each slot.

14   The MAC Channel use versus MACIndex shall be as specified in Table 9.3.1.3.2.1.3-1.

15   Symbols of each MAC Channel shall be transmitted on one of the Walsh channels. The MAC  
 16   channel gains may vary the relative power as a function of time. The orthogonal Walsh  
 17   channels shall be scaled to maintain a constant total transmit power. The sum of the  
 18   squares of the normalized gains on the orthogonal MAC Channels should equal one. The  
 19   Walsh Channel gains can vary as a function of time.

20   **Table 9.3.1.3.2.1.3-1. MAC Channel and Preamble Use Versus MACIndex**

MACIndex	MAC Channel Use	Preamble Use
0 and 1	Not Used	Not Used
2	Not Used	76.8-kbps Control Channel
3	Not Used	38.4-kbps Control Channel
4	RA Channel	Not Used
5–63	Available for RPC Channel Transmissions	Available for Forward Traffic Channel Transmissions

## 21   9.3.1.3.2.2.1 Reverse Power Control Channel

22   The Reverse Power Control (RPC) Channel for each access terminal with an open connection  
 23   shall be assigned to one of the available MAC Channels. It is used for the transmission of  
 24   the RPC bit stream destined to that access terminal.

1 The RPC data rate shall be 600 bps. Each RPC symbol shall be transmitted four times per  
 2 slot in bursts of 64 chips each. One burst shall be transmitted immediately preceding and  
 3 following each pilot burst in a slot as shown in Figure 9.3.1.3.1-2.

4 9.3.1.3.2.2.2 Reverse Activity Channel

5 The Reverse Activity (RA) Channel shall transmit the Reverse Activity Bit (RAB) stream over  
 6 the MAC Channel with MACIndex 4. The RA bit shall be transmitted over RABLength  
 7 successive slots. The transmission of each RA bit shall start in a slot that satisfies

$$8 \quad T \bmod RABLength = RABOffset,$$

9 where T is the system time in slots and RABLength and RABOffset are fields in the public  
 10 data TrafficChannelAssignment of the Route Update Protocol.

11 The RA Channel data rate shall be  $600/RABLength$  bps. Each RA bit shall be repeated and  
 12 transmitted over RABLength consecutive slots. The RA bit in each slot shall be further  
 13 repeated to form four symbols per slot for transmission.

14 9.3.1.3.2.3 Forward Traffic Channel

15 9.3.1.3.2.3.1 Forward Traffic Channel Preamble

16 A preamble sequence shall be transmitted with each Forward Traffic Channel and Control  
 17 Channel physical layer packet in order to assist the access terminal with synchronization of  
 18 each variable-rate transmission.

19 The preamble shall consist of all-'0' symbols transmitted on the in-phase component only.  
 20 The preamble shall be time multiplexed into the Forward Traffic Channel stream as  
 21 described in 9.3.1.3.3. The preamble sequence shall be covered by a 32-chip bi-orthogonal  
 22 sequence and the sequence shall be repeated several times depending on the transmit  
 23 mode. The bi-orthogonal sequence shall be specified in terms of the 32-ary Walsh functions  
 24 and their bit-by-bit complements by

$$25 \quad \begin{array}{c} W_{i/2}^{32} \text{ for } i = 0, 2, \dots, 62 \\ \hline W_{(i-1)/2}^{32} \text{ for } i = 1, 3, \dots, 63 \end{array}$$

26 where  $i = 0, 1, \dots, 63$  is the MACIndex value and  $\overline{W_i^{32}}$  is the bit-by-bit complement of the  
 27 32-chip Walsh function of order i.

28 The channel type versus MACIndex mapping for the preamble shall be as specified in Table  
 29 9.3.1.3.2.1.3-1.

30 The 32-chip preamble repetition factor shall be as specified in Table 9.3.1.3.2.3.1-1.

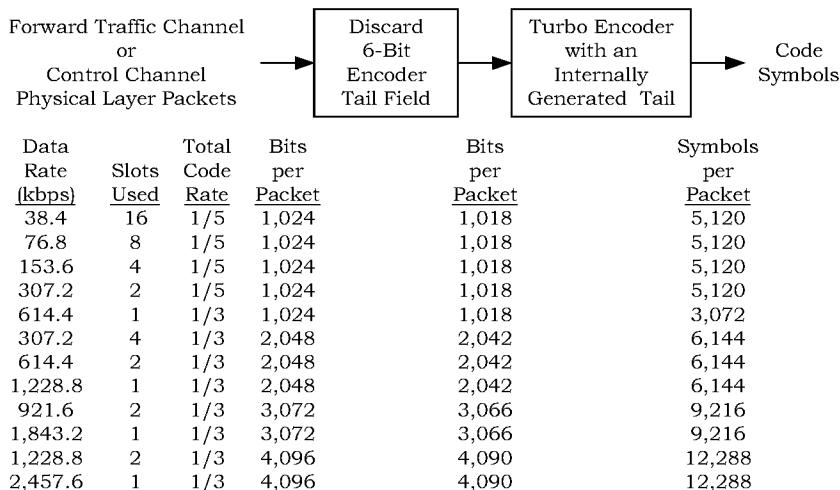
**Table 9.3.1.3.2.3.1-1. Preamble Repetition**

<b>Data Rate (kbps)</b>	<b>Values per Physical Layer Packet</b>		
	<b>Slots</b>	<b>32-Chip Preamble Sequence Repetitions</b>	<b>Preamble Chips</b>
38.4	16	32	1,024
76.8	8	16	512
153.6	4	8	256
307.2	2	4	128
614.4	1	2	64
307.2	4	4	128
614.4	2	2	64
1,228.8	1	2	64
921.6	2	2	64
1,843.2	1	2	64
1,228.8	2	2	64
2,457.6	1	2	64

### 9.3.1.3.2.3.2 Encoding

The Traffic Channel physical layer packets shall be encoded with code rates of  $R = 1/3$  or  $1/5$ . The encoder shall discard the 6-bit TAIL field of the physical layer packet inputs and encode the remaining bits with a parallel turbo encoder, as specified in 9.3.1.3.2.3.2.1. The turbo encoder will add an internally generated tail of  $6/R$  output code symbols, so that the total number of output symbols is  $1/R$  times the number of bits in the input physical layer packet.

Figure 9.3.1.3.2.3.2-1 illustrates the forward link encoding approach. The forward link encoder parameters shall be as specified in Table 9.3.1.3.2.3.2-1.

**Figure 9.3.1.3.2.3.2-1. Forward Link Encoder****Table 9.3.1.3.2.3.2-1. Parameters of the Forward Link Encoder**

Data Rate (kbps)	Values per Physical Layer Packet				
	Slots	Bits	Turbo Encoder Input Bits	Code Rate	Turbo Encoder Output Symbols
38.4	16	1,024	1,018	1/5	5,120
76.8	8	1,024	1,018	1/5	5,120
153.6	4	1,024	1,018	1/5	5,120
307.2	2	1,024	1,018	1/5	5,120
614.4	1	1,024	1,018	1/3	3,072
307.2	4	2,048	2,042	1/3	6,144
614.4	2	2,048	2,042	1/3	6,144
1,228.8	1	2,048	2,042	1/3	6,144
921.6	2	3,072	3,066	1/3	9,216
1,843.2	1	3,072	3,066	1/3	9,216
1,228.8	2	4,096	4,090	1/3	12,288
2,457.6	1	4,096	4,090	1/3	12,288

1

2

3

4

## 5    9.3.1.3.2.3.2.1 Turbo Encoder

6    The turbo encoder employs two systematic, recursive, convolutional encoders connected in  
7    parallel, with an interleaver, the turbo interleaver, preceding the second recursive  
8    convolutional encoder. The two recursive convolutional codes are called the constituent

1 codes of the turbo code. The outputs of the constituent encoders are punctured and  
 2 repeated to achieve the desired number of turbo encoder output symbols.

3 The transfer function for the constituent code shall be

$$4 \quad G(D) = \left[ 1 \quad \frac{n_0(D)}{d(D)} \quad \frac{n_1(D)}{d(D)} \right]$$

5 where  $d(D) = 1 + D^2 + D^3$ ,  $n_0(D) = 1 + D + D^3$ , and  $n_1(D) = 1 + D + D^2 + D^3$ .

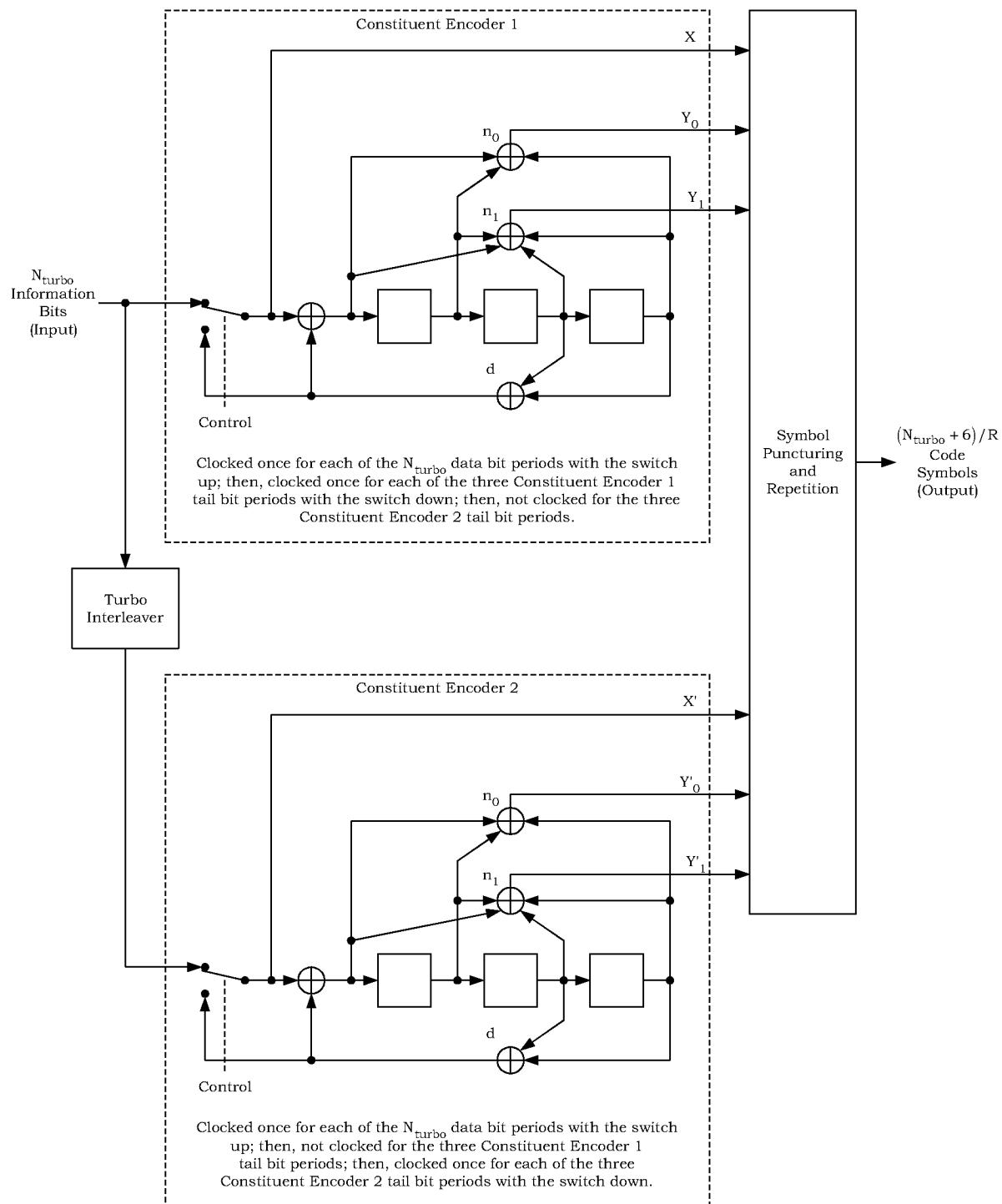
6 The turbo encoder shall generate an output symbol sequence that is identical to the one  
 7 generated by the encoder shown in Figure 9.3.1.3.2.3.2.1-1. Initially, the states of the  
 8 constituent encoder registers in this figure are set to zero. Then, the constituent encoders  
 9 are clocked with the switches in the positions noted.

10 Let  $N_{\text{turbo}}$  be the number of bits into the turbo encoder after the 6-bit physical layer packet  
 11 TAIL field is discarded. Then, the encoded data output symbols are generated by clocking  
 12 the constituent encoders  $N_{\text{turbo}}$  times with the switches in the up positions and puncturing  
 13 the outputs as specified in Table 9.3.1.3.2.3.2.1-1. Within a puncturing pattern, a '0' means  
 14 that the symbol shall be deleted and a '1' means that the symbol shall be passed. The  
 15 constituent encoder outputs for each bit period shall be output in the sequence  $X, Y_0, Y_1,$   
 16  $X', Y'_0, Y'_1$  with the  $X$  output first. Symbol repetition is not used in generating the encoded  
 17 data output symbols.

18 The turbo encoder shall generate 6/R tail output symbols following the encoded data output  
 19 symbols. This tail output symbol sequence shall be identical to the one generated by the  
 20 encoder shown in Figure 9.3.1.3.2.3.2.1-1. The tail output symbols are generated after the  
 21 constituent encoders have been clocked  $N_{\text{turbo}}$  times with the switches in the up position.

22 The first 3/R tail output symbols are generated by clocking Constituent Encoder 1 three  
 23 times with its switch in the down position while Constituent Encoder 2 is not clocked and  
 24 puncturing and repeating the resulting constituent encoder output symbols. The last 3/R  
 25 tail output symbols are generated by clocking Constituent Encoder 2 three times with its  
 26 switch in the down position while Constituent Encoder 1 is not clocked and puncturing and  
 27 repeating the resulting constituent encoder output symbols. The constituent encoder  
 28 outputs for each bit period shall be output in the sequence  $X, Y_0, Y_1, X', Y'_0, Y'_1$  with the  $X$   
 29 output first.

30 The constituent encoder output symbol puncturing for the tail symbols shall be as specified  
 31 in Table 9.3.1.3.2.3.2.1-2. Within a puncturing pattern, a '0' means that the symbol shall  
 32 be deleted and a '1' means that a symbol shall be passed. For rate-1/5 turbo codes, the tail  
 33 output code symbols for each of the first three tail bit periods shall be punctured and  
 34 repeated to achieve the sequence  $XXY_0Y_1Y_1$ , and the tail output code symbols for each of  
 35 the last three tail bit periods shall be punctured and repeated to achieve the sequence  
 36  $XX'Y'_0Y'_1Y'_1$ . For rate-1/3 turbo codes, the tail output symbols for each of the first three  
 37 tail bit periods shall be  $XXY_0$ , and the tail output symbols for each of the last three tail bit  
 38 periods shall be  $XX'Y'_0$ .

**Figure 9.3.1.3.2.3.2.1-1. Turbo Encoder**

**Table 9.3.1.3.2.3.2.1-1. Puncturing Patterns for the Data Bit Periods**

<b>Output</b>	<b>Code Rate</b>	
	<b>1/3</b>	<b>1/5</b>
X	1	1
Y <sub>0</sub>	1	1
Y <sub>1</sub>	0	1
X'	0	0
Y' <sub>0</sub>	1	1
Y' <sub>1</sub>	0	1

Note: For each rate, the puncturing table shall be read from top to bottom.

2

3

**Table 9.3.1.3.2.3.2.1-2. Puncturing Patterns for the Tail Bit Periods**

<b>Output</b>	<b>Code Rate</b>	
	<b>1/3</b>	<b>1/5</b>
X	111 000	111 000
Y <sub>0</sub>	111 000	111 000
Y <sub>1</sub>	000 000	111 000
X'	000 111	000 111
Y' <sub>0</sub>	000 111	000 111
Y' <sub>1</sub>	000 000	000 111

Note: For rate-1/3 turbo codes, the puncturing table shall be read first from top to bottom repeating X and X', and then from left to right. For rate-1/5 turbo codes, the puncturing table shall be read first from top to bottom repeating X, X', Y<sub>1</sub>, and Y'<sub>1</sub> and then from left to right.

4

5

### 9.3.1.3.2.3.2.2 Turbo Interleaver

6

7

The turbo interleaver, which is part of the turbo encoder, shall block interleave the turbo encoder input data that is fed to Constituent Encoder 2.

8

9

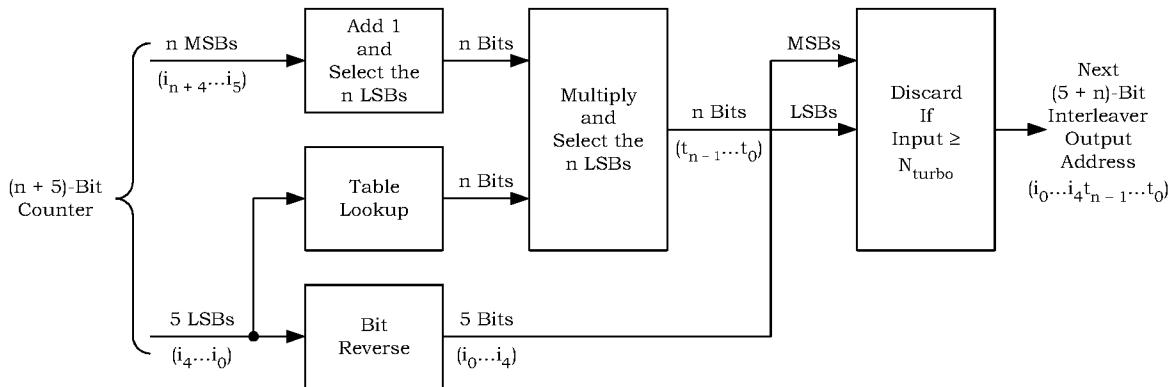
10

11

The turbo interleaver shall be functionally equivalent to an approach where the entire sequence of turbo interleaver input bits are written sequentially into an array at a sequence of addresses, and then the entire sequence is read out from a sequence of addresses that are defined by the procedure described below.

Let the sequence of input addresses be from 0 to  $N_{\text{turbo}} - 1$ . Then, the sequence of interleaver output addresses shall be equivalent to those generated by the procedure illustrated in Figure 9.3.1.3.2.3.2.2-1 and described below.<sup>47</sup>

1. Determine the turbo interleaver parameter,  $n$ , where  $n$  is the smallest integer such that  $N_{\text{turbo}} \leq 2^{n+5}$ . Table 9.3.1.3.2.3.2.2-1 gives this parameter for the different physical layer packet sizes.
2. Initialize an  $(n + 5)$ -bit counter to 0.
3. Extract the  $n$  most significant bits (MSBs) from the counter and add one to form a new value. Then, discard all except the  $n$  least significant bits (LSBs) of this value.
4. Obtain the  $n$ -bit output of the table lookup defined in Table 9.3.1.3.2.3.2.2-2 with a read address equal to the five LSBs of the counter. Note that this table depends on the value of  $n$ .
5. Multiply the values obtained in Steps 3 and 4, and discard all except the  $n$  LSBs.
6. Bit-reverse the five LSBs of the counter.
7. Form a tentative output address that has its MSBs equal to the value obtained in Step 6 and its LSBs equal to the value obtained in Step 5.
8. Accept the tentative output address as an output address if it is less than  $N_{\text{turbo}}$ ; otherwise, discard it.
9. Increment the counter and repeat Steps 3 through 8 until all  $N_{\text{turbo}}$  interleaver output addresses are obtained.



**Figure 9.3.1.3.2.3.2.2-1. Turbo Interleaver Output Address Calculation Procedure**

<sup>47</sup> This procedure is equivalent to one where the counter values are written into a  $2^5$ -row by  $2^n$ -column array by rows, the rows are shuffled according to a bit-reversal rule, the elements within each row are permuted according to a row-specific linear congruential sequence, and tentative output addresses are read out by column. The linear congruential sequence rule is  $x(i + 1) = (x(i) + c) \bmod 2^n$ , where  $x(0) = c$  and  $c$  is a row-specific value from a table lookup.

**Table 9.3.1.3.2.3.2.2-1. Turbo Interleaver Parameter**

<b>Physical Layer Packet Size</b>	<b>Turbo Interleaver Block Size <math>N_{turbo}</math></b>	<b>Turbo Interleaver Parameter <math>n</math></b>
1,024	1,018	5
2,048	2,042	6
3,072	3,066	7
4,096	4,090	7

2

1

**Table 9.3.1.3.2.3.2.2-2. Turbo Interleaver Lookup Table Definition**

<b>Table Index</b>	<b>n = 5 Entries</b>	<b>n = 6 Entries</b>	<b>n = 7 Entries</b>
0	27	3	15
1	3	27	127
2	1	15	89
3	15	13	1
4	13	29	31
5	17	5	15
6	23	1	61
7	13	31	47
8	9	3	127
9	3	9	17
10	15	15	119
11	3	31	15
12	13	17	57
13	1	5	123
14	13	39	95
15	29	1	5
16	21	19	85
17	19	27	17
18	1	15	55
19	3	13	57
20	29	45	15
21	17	5	41
22	25	33	93
23	29	15	87
24	9	13	63
25	13	9	15
26	23	15	13
27	13	31	15
28	13	17	81
29	1	5	57
30	13	15	31
31	13	33	69

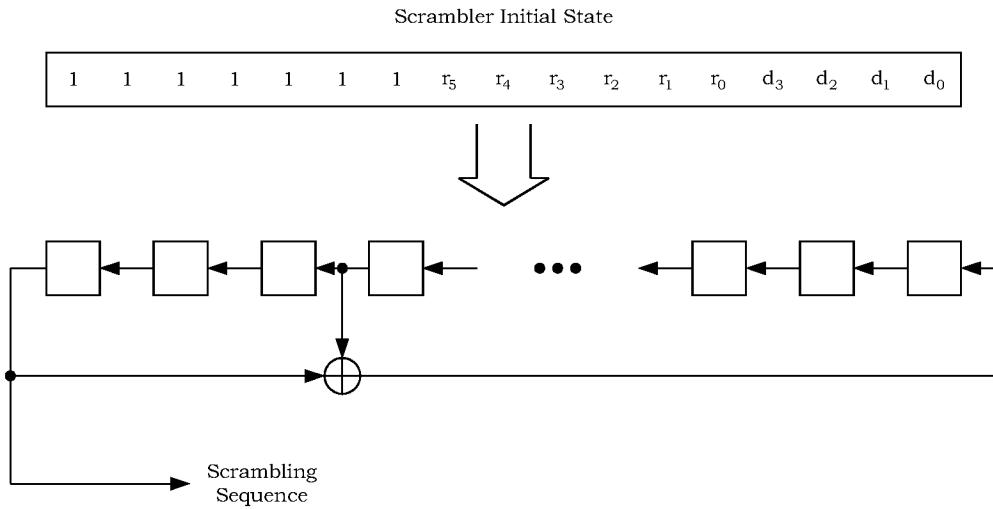
2

## 1    9.3.1.3.2.3.3 Scrambling

2    The output of the encoder shall be scrambled to randomize the data prior to modulation.  
 3    The scrambling sequence shall be equivalent to one generated with a 17-tap linear feedback  
 4    shift register with a generator sequence of  $h(D) = D^{17} + D^{14} + 1$ , as shown in Figure  
 5    9.3.1.3.2.3.3-1. At the start of the physical layer packet, the shift register shall be initialized  
 6    to the state [111111r<sub>5</sub>r<sub>4</sub>r<sub>3</sub>r<sub>2</sub>r<sub>1</sub>r<sub>0</sub>d<sub>3</sub>d<sub>2</sub>d<sub>1</sub>d<sub>0</sub>]. The r<sub>5</sub>r<sub>4</sub>r<sub>3</sub>r<sub>2</sub>r<sub>1</sub>r<sub>0</sub> bits shall be equal to the 6-  
 7    bit preamble MACIndex value (see Table 9.3.1.3.2.1.3-1). The d<sub>3</sub>d<sub>2</sub>d<sub>1</sub>d<sub>0</sub> bits shall be  
 8    determined by the data rate, as specified in Table 9.3.1.3.2.3.3-1. The initial state shall  
 9    generate the first scrambling bit. The shift register shall be clocked once for every encoder  
 10   output code symbol to generate a bit of the scrambling sequence. Every encoder output  
 11   code symbol shall be XOR'd with the corresponding bit of the scrambling sequence to yield  
 12   a scrambled encoded bit.

13    **Table 9.3.1.3.2.3.3-1. Parameters Controlling the Scrambler Initial State**

Data Rate (kbps)	Slots per Physical Layer Packet	d <sub>3</sub>	d <sub>2</sub>	d <sub>1</sub>	d <sub>0</sub>
38.4	16	0	0	0	1
76.8	8	0	0	1	0
153.6	4	0	0	1	1
307.2	2	0	1	0	0
307.2	4	0	1	0	1
614.4	1	0	1	1	0
614.4	2	0	1	1	1
921.6	2	1	0	0	0
1,228.8	1	1	0	0	1
1,228.8	2	1	0	1	0
1,843.2	1	1	0	1	1
2,457.6	1	1	1	0	0



**Figure 9.3.1.3.2.3.3-1. Symbol Scrambler**

### 9.3.1.3.2.3.4 Channel Interleaving

The channel interleaving shall consist of a symbol reordering followed by symbol permuting.

#### 9.3.1.3.2.3.4.1 Symbol Reordering

The scrambled turbo encoder data and tail output symbols generated with the rate-1/5 encoder shall be reordered according to the following procedure:

1. All of the scrambled data and tail turbo encoder output symbols shall be demultiplexed into five sequences denoted  $U$ ,  $V_0$ ,  $V_1$ ,  $V'_0$ , and  $V'_1$ . The scrambled encoder output symbols shall be sequentially distributed from the  $U$  sequence to the  $V'_1$  sequence with the first scrambled encoder output symbol going to the  $U$  sequence, the second to the  $V_0$  sequence, the third to the  $V_1$  sequence, the fourth to the  $V'_0$  sequence, the fifth to the  $V'_1$  sequence, the sixth to the  $U$  sequence, etc.
2. The  $U$ ,  $V_0$ ,  $V_1$ ,  $V'_0$ , and  $V'_1$  sequences shall be ordered according to  $UV_0V'_0V_1V'_1$ . That is, the  $U$  sequence of symbols shall be first and the  $V'_1$  sequence of symbols shall be last.

The scrambled turbo encoder data and tail output symbols generated with the rate-1/3 encoder shall be reordered according to the following procedure:

1. All of the scrambled data and tail turbo encoder output symbols shall be demultiplexed into three sequences denoted  $U$ ,  $V_0$ , and  $V'_0$ . The scrambled encoder output symbols shall be sequentially distributed from the  $U$  sequence to the  $V'_0$  sequence with the first scrambled encoder output symbol going to the  $U$  sequence, the second to the  $V_0$  sequence, the third to the  $V'_0$  sequence, the fourth to the  $U$  sequence, etc.
2. The  $U$ ,  $V_0$ , and  $V'_0$  sequences shall be ordered according to  $UV_0V'_0$ . That is, the  $U$  sequence of symbols shall be first and the  $V'_0$  sequence of symbols shall be last.

Table 9.3.1.3.2.3.4.1-1 gives the order of the symbols out of the turbo encoder and their mapping to demultiplexer output sequences. The encoder output symbol notation is used, but the encoder output symbols are scrambled before the reordering demultiplexer.

**Table 9.3.1.3.2.3.4.1-1. Scrambled Turbo Encoder Output and Symbol Reordering Demultiplexer Symbol Sequences**

<b>Type of Sequence</b>	<b>Symbol Sequence</b>	
	<b>R = 1/5</b>	<b>R = 1/3</b>
Turbo Encoder Data Output Sequence	X Y <sub>0</sub> Y <sub>1</sub> Y' <sub>0</sub> Y' <sub>1</sub>	X Y <sub>0</sub> Y' <sub>0</sub>
Turbo Encoder Constituent Encoder 1 Tail Output Sequence	X X Y <sub>0</sub> Y <sub>1</sub> Y <sub>1</sub>	X X Y <sub>0</sub>
Turbo Encoder Constituent Encoder 2 Tail Output Sequence	X' X' Y' <sub>0</sub> Y' <sub>1</sub> Y' <sub>1</sub>	X' X' Y' <sub>0</sub>
Demultiplexer Output Sequence	U V <sub>0</sub> V' <sub>0</sub> V <sub>1</sub> V' <sub>1</sub>	U V <sub>0</sub> V' <sub>0</sub>

### 9.3.1.3.2.3.4.2 Symbol Permuting

The reordered symbols shall be permuted in three separate bit-reversal interleaver blocks with rate-1/5 coding and in two separate blocks with rate-1/3 coding. The permuter input blocks shall consist of the sequence of U symbols, the sequence of V<sub>0</sub> and V'<sub>0</sub> symbols (denoted as V<sub>0</sub>/V'<sub>0</sub>), and, with rate-1/5 coding, the sequence of V<sub>1</sub> and V'<sub>1</sub> symbols (denoted as V<sub>1</sub>/V'<sub>1</sub>).

The sequence of interleaver output symbols for the blocks shall be equivalent to those generated by the procedure described below with the parameters specified in Table 9.3.1.3.2.3.4.2-1:

1. Write the entire sequence of symbols in the input block into a rectangular array of K rows and M columns. Write the symbols in by rows starting from the top row, writing the rows from left to right.
2. Label the columns of the array by the index j, where j = 0,..., M - 1 and column 0 is the left-most column. Then, end-around shift the symbols of each column downward by  $j \bmod K$  for the U block and by  $\lfloor j/4 \rfloor \bmod K$  for the V<sub>0</sub>/V'<sub>0</sub> and V<sub>1</sub>/V'<sub>1</sub> blocks.
3. Reorder the columns such that column j is moved to column BRO(j), where BRO(j) indicates the bit-reversed value of j. For example, for M = 512, BRO(6) = 192.
4. Read the entire array of symbols out by columns starting from the left-most column, reading the columns from top to bottom.

- With rate-1/5 coding, the interleaver output sequence shall be the interleaved U symbols followed by the interleaved  $V_0/V'_0$  symbols followed by the interleaved  $V_1/V'_1$  symbols.
- With rate-1/3 coding, the interleaver output sequence shall be the interleaved U symbols followed by the interleaved  $V_0/V'_0$ .

**Table 9.3.1.3.2.3.4.2-1. Channel Interleaver Parameters**

<b>Physical Layer Packet Size</b>	<b>U Block Interleaver Parameters</b>		<b><math>V_0/V'_0</math> and <math>V_1/V'_1</math> Block Interleaver Parameters</b>	
	<b>K</b>	<b>M</b>	<b>K</b>	<b>M</b>
1,024	2	512	2	1,024
2,048	2	1,024	2	2,048
3,072	3	1,024	3	2,048
4,096	4	1,024	4	2,048

- 9.3.1.3.2.3.5 Modulation
- The output of the channel interleaver shall be applied to a modulator that outputs an in-phase stream and a quadrature stream of modulated values. The modulator generates QPSK, 8-PSK, or 16-QAM modulation symbols, depending on the data rate.

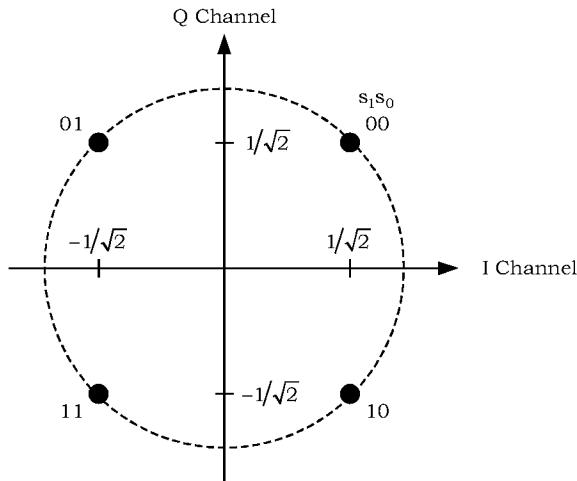
#### 9.3.1.3.2.3.5.1 QPSK Modulation

For physical layer packet sizes of 1,024 or 2,048 bits, groups of two successive channel interleaver output symbols shall be grouped to form QPSK modulation symbols. Each group of two adjacent block interleaver output symbols,  $x(2i)$  and  $x(2i + 1)$ ,  $i = 0, \dots, M - 1$  as specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol  $(m_I(i), m_Q(i))$  as specified in Table 9.3.1.3.2.3.5.1-1. Figure 9.3.1.3.2.3.5.1-1 shows the signal constellation of the QPSK modulator, where  $s_0 = x(2k)$  and  $s_1 = x(2k + 1)$ .

**Table 9.3.1.3.2.3.5.1-1. QPSK Modulation Table**

<b>Interleaved Symbols</b>		<b>Modulation Symbols</b>	
<b><math>s_1</math> <math>x(2k + 1)</math></b>	<b><math>s_0</math> <math>x(2k)</math></b>	<b><math>m_I(k)</math></b>	<b><math>m_Q(k)</math></b>
0	0	D	D
0	1	-D	D
1	0	D	-D
1	1	-D	-D

Note:  $D = 1/\sqrt{2}$ .



1

2

**Figure 9.3.1.3.2.3.5.1-1. Signal Constellation for QPSK Modulation**

## 3      9.3.1.3.2.3.5.2 8-PSK Modulation

4      For physical layer packet sizes of 3,072 bits, groups of three successive channel interleaver  
 5      output symbols shall be grouped to form 8-PSK modulation symbols. Each group of three  
 6      adjacent block interleaver output symbols,  $x(3i)$ ,  $x(3i + 1)$ , and  $x(3i + 2)$ ,  $i = 0, \dots, M - 1$  as  
 7      specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol  
 8       $(m_I(i), m_Q(i))$  as specified in Table 9.3.1.3.2.3.5.2-1. Figure 9.3.1.3.2.3.5.2-1 shows the  
 9      signal constellation of the 8-PSK modulator, where  $s_0 = x(3k)$ ,  $s_1 = x(3k + 1)$ , and  $s_2 = x(3k$   
 10      $+ 2)$ .

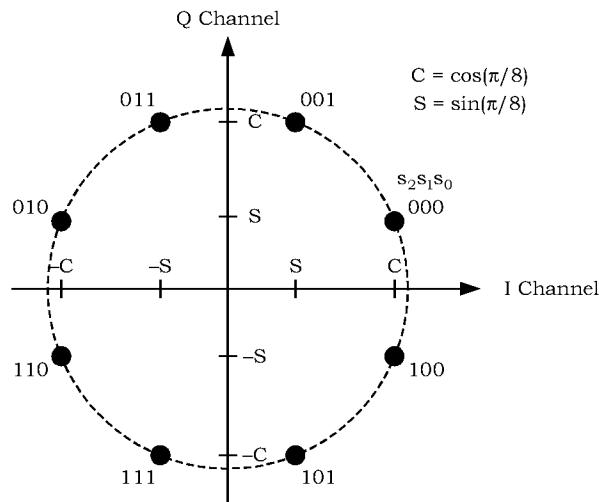
11

**Table 9.3.1.3.2.3.5.2-1. 8-PSK Modulation Table**

Interleaved Symbols			Modulation Symbols	
$s_2$ $x(3k + 2)$	$s_1$ $x(3k + 1)$	$s_0$ $x(3k)$	$m_I(k)$	$m_Q(k)$
0	0	0	C	S
0	0	1	S	C
0	1	1	-S	C
0	1	0	-C	S
1	1	0	-C	-S
1	1	1	-S	-C
1	0	1	S	-C
1	0	0	C	-S

Note:  $C = \cos(\pi/8) \approx 0.9239$  and  $S = \sin(\pi/8) \approx 0.3827$ .

12



**Figure 9.3.1.3.2.3.5.2-1. Signal Constellation for 8-PSK Modulation**

### 9.3.1.3.2.3.5.3 16-QAM Modulation

For physical layer packet sizes of 4,096 bits, groups of four successive channel interleaver output symbols shall be grouped to form 16-QAM modulation symbols. Each group of four adjacent block interleaver output symbols,  $x(4i)$ ,  $x(4i + 1)$ ,  $x(4i + 2)$ , and  $x(4i + 3)$ ,  $i = 0, \dots, M - 1$  as specified in Table 9.3.1.3.2.3.4.2-1, shall be mapped into a complex modulation symbol  $(m_I(i), m_Q(i))$  as specified in Table 9.3.1.3.2.3.5.3-1. Figure 9.3.1.3.2.3.5.3-1 shows the signal constellation of the 16QAM modulator, where  $s_0 = x(4k)$ ,  $s_1 = x(4k + 1)$ ,  $s_2 = x(4k + 2)$ , and  $s_3 = x(4k + 3)$ .

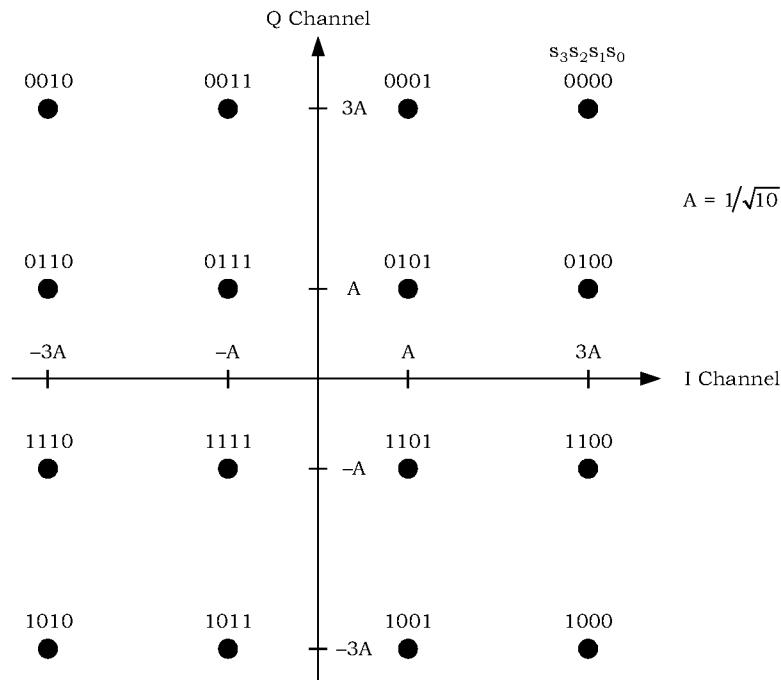
1

**Table 9.3.1.3.2.3.5.3-1. 16-QAM Modulation Table**

Interleaved Symbols				Modulation Symbols	
$s_3$ $x(4k + 3)$	$s_2$ $x(4k + 2)$	$s_1$ $x(4k + 1)$	$s_0$ $x(4k)$	$m_Q(k)$	$m_I(k)$
0	0	0	0	3A	3A
0	0	0	1	3A	A
0	0	1	1	3A	-A
0	0	1	0	3A	-3A
0	1	0	0	A	3A
0	1	0	1	A	A
0	1	1	1	A	-A
0	1	1	0	A	-3A
1	1	0	0	-A	3A
1	1	0	1	-A	A
1	1	1	1	-A	-A
1	1	1	0	-A	-3A
1	0	0	0	-3A	3A
1	0	0	1	-3A	A
1	0	1	1	-3A	-A
1	0	1	0	-3A	-3A

Note:  $A = 1/\sqrt{10} \approx 0.3162$ .

2



**Figure 9.3.1.3.2.3.5.3-1. Signal Constellation for 16-QAM Modulation**

### 9.3.1.3.2.3.6 Sequence Repetition and Symbol Puncturing

Table 9.3.1.3.2.3.6-1 gives the number of modulation symbols that the modulator provides per physical layer packet and the number of modulation symbols needed for the data portion of the allocated slots. If the number of required modulation symbols is more than the number provided, the complete sequence of input modulation symbols shall be repeated as many full-sequence times as possible followed by a partial transmission if necessary. If a partial transmission is needed, the first portion of the input modulation symbol sequence shall be used. If the number of required modulation symbols is less than the number provided, only the first portion of the input modulation symbol sequence shall be used.

The sequence repetition and symbol puncturing parameters shall be as specified in Table 9.3.1.3.2.3.6-1. The entries in the column labeled "Number of Modulation Symbols Needed" are equal to the number of data TDM chips given in Table 9.3.1.3.1.1-1 and Table 9.3.1.3.1.1-2.

**Table 9.3.1.3.2.3.6-1. Sequence Repetition and Symbol Puncturing Parameters**

Data Rate (kbps)	Values per Physical Layer Packet						Approximate Coding	
	Number of Slots	Number of Bits	Number of Modulation Symbols Provided	Number of Modulation Symbols Needed	Number of Full Sequence Transmissions	Number of Modulation Symbols in Last Partial Transmission	Code Rate	Repetition Factor
38.4	16	1,024	2,560	24,576	9	1,536	1/5	9.6
76.8	8	1,024	2,560	12,288	4	2,048	1/5	4.8
153.6	4	1,024	2,560	6,144	2	1,024	1/5	2.4
307.2	2	1,024	2,560	3,072	1	512	1/5	1.2
614.4	1	1,024	1,536	1,536	1	0	1/3	1
307.2	4	2,048	3,072	6,272	2	128	1/3	2.04
614.4	2	2,048	3,072	3,136	1	64	1/3	1.02
1,228.8	1	2,048	3,072	1,536	0	1,536	2/3	1
921.6	2	3,072	3,072	3,136	1	64	1/3	1.02
1,843.2	1	3,072	3,072	1,536	0	1,536	2/3	1
1,228.8	2	4,096	3,072	3,136	1	64	1/3	1.02
2,457.6	1	4,096	3,072	1,536	0	1,536	2/3	1

2

### 3 9.3.1.3.2.3.7 Symbol Demultiplexing

4 The in-phase stream at the output of the sequence repetition operation shall be  
 5 demultiplexed into 16 parallel streams labeled  $I_0, I_1, I_2, \dots, I_{15}$ . If  $m_I(0), m_I(1), m_I(2), m_I(3), \dots$   
 6 denotes the sequence of sequence-repeated modulation output values in the in-phase  
 7 stream, then for each  $k = 0, 1, 2, \dots, 15$ , the  $k^{\text{th}}$  demultiplexed stream  $I_k$  shall consist of the  
 8 values  $m_I(k), m_I(16 + k), m_I(32 + k), m_I(48 + k), \dots$

9 Similarly, the quadrature stream at the output of the sequence repetition operation shall be  
 10 demultiplexed into 16 parallel streams labeled  $Q_0, Q_1, Q_2, \dots, Q_{15}$ . If  $m_Q(0), m_Q(1), m_Q(2), m_Q(3), \dots$   
 11 denotes the sequence of sequence-repeated modulation output values in the  
 12 quadrature stream, then for each  $k = 0, 1, 2, \dots, 15$ , the  $k^{\text{th}}$  demultiplexed stream  $Q_k$  shall  
 13 consist of the values  $m_Q(k), m_Q(16 + k), m_Q(32 + k), m_Q(48 + k), \dots$

14 Each demultiplexed stream at the output of the symbol demultiplexer shall consist of  
 15 modulation values at the rate of 76.8 ksps.

1    9.3.1.3.2.3.8 Walsh Channel Assignment

2    The individual streams generated by the symbol demultiplexer shall be assigned to one of  
3    16 distinct Walsh channels. For each  $k = 0, 1, 2, \dots, 15$ , the demultiplexed streams with  
4    labels  $I_k$  and  $Q_k$  shall be assigned to the in-phase and quadrature phases, respectively, of  
5    the  $k^{\text{th}}$  Walsh channel  $W_k^{16}$ . The modulation values associated with the in-phase and  
6    quadrature phase components of the same Walsh channel are referred to as Walsh  
7    symbols.

8    9.3.1.3.2.3.9 Walsh Channel Scaling

9    The modulated symbols on each branch of each Walsh channel shall be scaled to maintain  
10   a constant total transmit power independent of data rate. For this purpose, each orthogonal  
11   channel shall be scaled by a gain of  $\frac{1}{\sqrt{16}} = \frac{1}{4}$ . The gain settings are normalized to a unity  
12   reference equivalent to unmodulated BPSK transmitted at full power.

13   9.3.1.3.2.3.10 Walsh Chip Level Summing

14   The scaled Walsh chips associated with the 16 Walsh channels shall be summed on a chip-  
15   by-chip basis.

16   9.3.1.3.2.4 Control Channel

17   The Control Channel transmits broadcast messages and access-terminal-directed  
18   messages. The Control Channel messages shall be transmitted at a data rate of 76.8 kbps  
19   or 38.4 kbps. The modulation characteristics shall be the same as those of the Forward  
20   Traffic Channel at the corresponding data rate. The Control Channel transmissions shall be  
21   distinguished from Forward Traffic Channel transmissions by having a preamble that is  
22   covered by a bi-orthogonal cover sequence with MACIndex 2 or 3, as specified in  
23   9.3.1.3.2.3.1. A MACIndex value of 2 shall be used for the 76.8-kbps data rate, and a  
24   MACIndex value of 3 shall be used for the 38.4-kbps data rate.

25   9.3.1.3.3 Time-Division Multiplexing

26   The Forward Traffic Channel or Control Channel data modulation chips shall be time-  
27   division multiplexed with the preamble, Pilot Channel, and MAC Channel chips according to  
28   the timing diagrams in Figure 9.3.1.3.3-1, Figure 9.3.1.3.3-2, Figure 9.3.1.3.3-3, and  
29   Figure 9.3.1.3.3-4. The multiplexing parameters shall be as specified in Table 9.3.1.3.3-1.

30   The Walsh chip rate shall be fixed at 1.2288 Mcps.

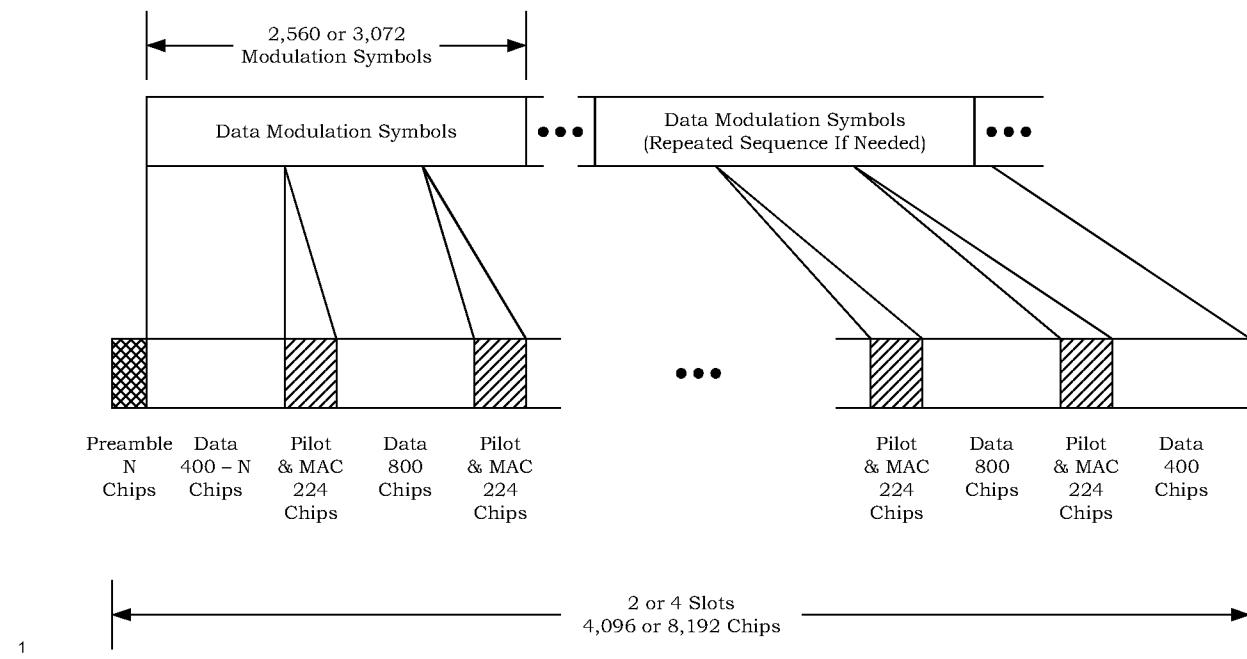


Figure 9.3.1.3.3-1. Preamble, Pilot, MAC, and Data Multiplexing for the Multiple-Slot Cases with Data Rates of 153.6, 307.2, 614.4, 921.6, and 1228.8 kbps

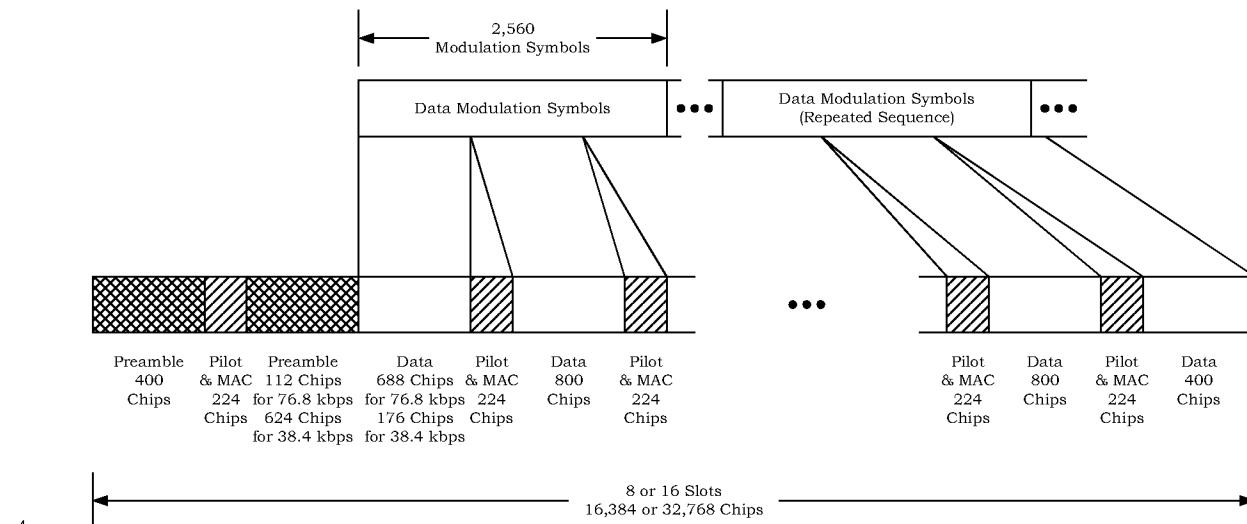
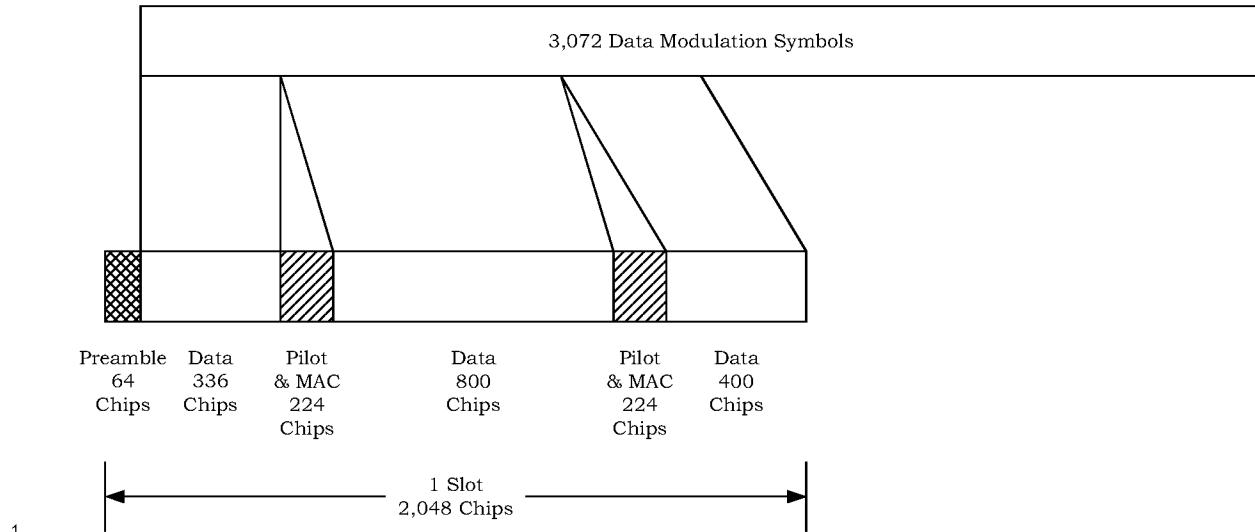
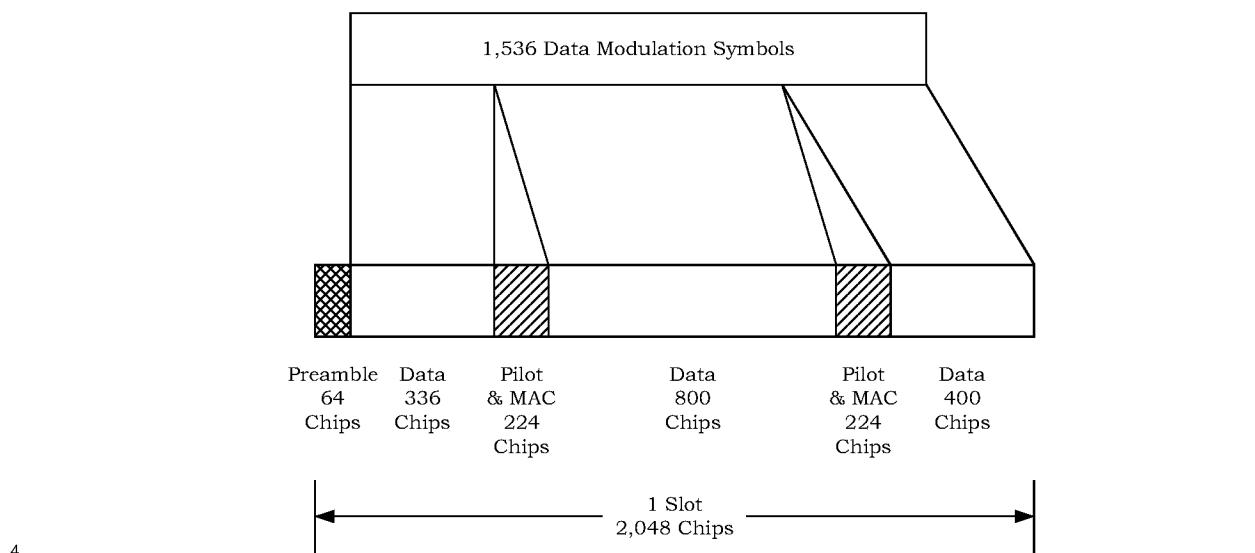


Figure 9.3.1.3.3-2. Preamble, Pilot, MAC, and Data Multiplexing with Data Rates of 38.4 and 76.8 kbps



**Figure 9.3.1.3.3-3. Preamble, Pilot, MAC, and Data Multiplexing for the 1-Slot Cases with Data Rates of 1.2288, 1.8432, and 2.4576 Mbps**



**Figure 9.3.1.3.3-4. Preamble, Pilot, MAC, and Data Multiplexing for the 1-Slot Case with a Data Rate of 614.4 kbps**

**Table 9.3.1.3.3-1. Preamble, Pilot, MAC, and Data Multiplexing Parameters**

Data Rate (kbps)	Number of Values per Physical Layer Packet					
	Slots	Bits	Preamble Chips	Pilot Chips	MAC Chips	Data Chips
38.4	16	1,024	1,024	3,072	4,096	24,576
76.8	8	1,024	512	1,536	2,048	12,288
153.6	4	1,024	256	768	1,024	6,144
307.2	2	1,024	128	384	512	3,072
614.4	1	1,024	64	192	256	1,536
307.2	4	2,048	128	768	1,024	6,272
614.4	2	2,048	64	384	512	3,136
1,228.8	1	2,048	64	192	256	1,536
921.6	2	3,072	64	384	512	3,136
1,843.2	1	3,072	64	192	256	1,536
1,228.8	2	4,096	64	384	512	3,136
2,457.6	1	4,096	64	192	256	1,536

### 9.3.1.3.4 Quadrature Spreading

Following orthogonal spreading, the combined modulation sequence shall be quadrature spread as shown in Figure 9.3.1.3.1-1. The spreading sequence shall be a quadrature sequence of length  $2^{15}$  (i.e., 32768 PN chips in length). This sequence is called the pilot PN sequence and shall be based on the following characteristic polynomials:

$$P_I(x) = x^{15} + x^{10} + x^8 + x^7 + x^6 + x^2 + 1$$

(for the in-phase (I) sequence)

and

$$P_Q(x) = x^{15} + x^{12} + x^{11} + x^{10} + x^9 + x^5 + x^4 + x^3 + 1$$

(for the quadrature-phase (Q) sequence).

The maximum length linear feedback shift-register sequences  $\{I(n)\}$  and  $\{Q(n)\}$  based on the above polynomials are of length  $2^{15} - 1$  and can be generated by the following linear recursions:

$$I(n) = I(n - 15) \oplus I(n - 13) \oplus I(n - 9) \oplus I(n - 8) \oplus I(n - 7) \oplus I(n - 5)$$

(based on  $P_I(x)$  as the characteristic polynomial)

and

$$1 \quad Q(n) = Q(n - 15) \oplus Q(n - 12) \oplus Q(n - 11) \oplus Q(n - 10) \oplus Q(n - 6) \oplus Q(n - 5) \oplus$$

$$2 \quad Q(n - 4) \oplus Q(n - 3)$$

3 (based on  $P_Q(x)$  as the characteristic polynomial),

4 where  $I(n)$  and  $Q(n)$  are binary valued ('0' and '1') and the additions are modulo-2. In order  
 5 to obtain the  $I$  and  $Q$  pilot PN sequences (of period  $2^{15}$ ), a '0' is inserted in the  $\{I(n)\}$  and  
 6  $\{Q(n)\}$  sequences after 14 consecutive '0' outputs (this occurs only once in each period).  
 7 Therefore, the pilot PN sequences have one run of 15 consecutive '0' outputs instead of 14.

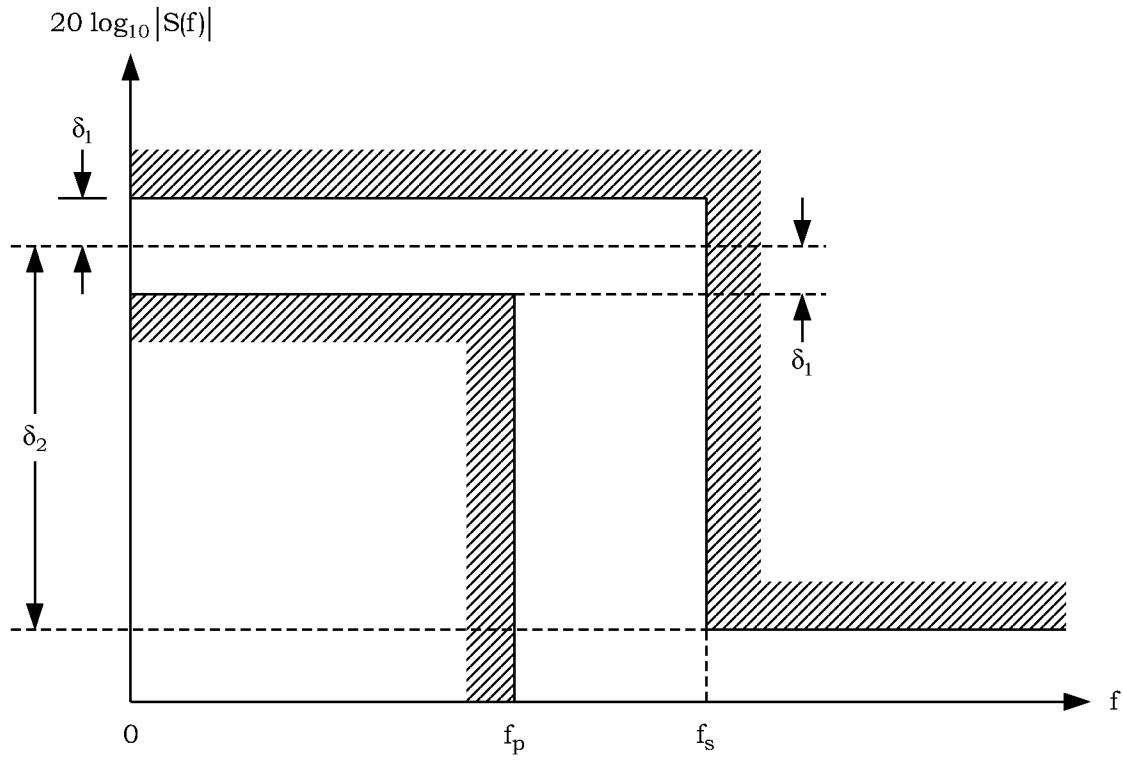
8 The chip rate for the pilot PN sequence shall be 1.2288Mcps. The pilot PN sequence period  
 9 is  $32768/1228800 = 26.666\dots$  ms, and exactly 75 pilot PN sequence repetitions occur every  
 10 2 seconds.

11 Pilot Channels shall be identified by an offset index in the range from 0 through 511  
 12 inclusive. This offset index shall specify the offset value (in units of 64 chips) of the pilot PN  
 13 sequence from the zero-offset pilot PN sequence. The zero-offset pilot PN sequence shall be  
 14 such that the start of the sequence shall be output at the beginning of every even second in  
 15 time, referenced to access network transmission time. The start of the zero-offset pilot PN  
 16 sequence for either the  $I$  or  $Q$  sequences shall be defined as the state of the sequence for  
 17 which the next 15 outputs inclusive are '0'. Equivalently, the zero-offset sequence is defined  
 18 such that the last chip prior to the even-second mark as referenced to the transmit time  
 19 reference is a '1' prior to the 15 consecutive '0's.

#### 20 9.3.1.3.5 Filtering

##### 21 9.3.1.3.5.1 Baseband Filtering

22 Following the quadrature spreading operation, the  $I'$  and  $Q'$  impulses are applied to the  
 23 inputs of the  $I$  and  $Q$  baseband filters as shown in Figure 9.3.1.3.1-1. The baseband filters  
 24 shall have a frequency response  $S(f)$  that satisfies the limits given in Figure 9.3.1.3.5.1-1.  
 25 Specifically, the normalized frequency response of the filter shall be contained within  $\pm\delta_1$  in  
 26 the passband  $0 \leq f \leq f_p$  and shall be less than or equal to  $-\delta_2$  in the stopband  $f \geq f_s$ . The  
 27 numerical values for the parameters are  $\delta_1 = 1.5$  dB,  $\delta_2 = 40$  dB,  $f_p = 590$  kHz, and  $f_s = 740$   
 28 kHz.



**Figure 9.3.1.3.5.1-1. Baseband Filter Frequency Response Limits**

The impulse response of the baseband filter,  $s(t)$ , should satisfy the following equation:

$$\text{Mean Squared Error} = \sum_{k=0}^{\infty} [\alpha s(kT_s - \tau) - h(k)]^2 \leq 0.03,$$

where the constants  $\alpha$  and  $\tau$  are used to minimize the mean squared error. The constant  $T_s$  is equal to 203.451... ns, which equals one quarter of a PN chip. The values of the coefficients  $h(k)$ , for  $k < 48$ , are given in Table 9.3.1.3.5.1-1;  $h(k) = 0$  for  $k \geq 48$ . Note that  $h(k)$  equals  $h(47 - k)$ .

1

**Table 9.3.1.3.5.1-1. Baseband Filter Coefficients**

<b>k</b>	<b>h(k)</b>
0, 47	-0.025288315
1, 46	-0.034167931
2, 45	-0.035752323
3, 44	-0.016733702
4, 43	0.021602514
5, 42	0.064938487
6, 41	0.091002137
7, 40	0.081894974
8, 39	0.037071157
9, 38	-0.021998074
10, 37	-0.060716277
11, 36	-0.051178658
12, 35	0.007874526
13, 34	0.084368728
14, 33	0.126869306
15, 32	0.094528345
16, 31	-0.012839661
17, 30	-0.143477028
18, 29	-0.211829088
19, 28	-0.140513128
20, 27	0.094601918
21, 26	0.441387140
22, 25	0.785875640
23, 24	1.0

2

## 3    9.3.1.3.5.2 Phase Characteristics

4    The access network shall provide phase equalization for the transmit signal path.<sup>48</sup> The  
5    equalizing filter shall be designed to provide the equivalent baseband transfer function

---

<sup>48</sup>This equalization simplifies the design of the access terminal receive filters.

$$H(\omega) = K \frac{\omega^2 + j\alpha\omega\omega_0 - \omega_0^2}{\omega^2 - j\alpha\omega\omega_0 - \omega_0^2},$$

where  $K$  is an arbitrary gain,  $j$  equals  $\sqrt{-1}$ ,  $\alpha$  equals 1.36,  $\omega_0$  equals  $2\pi \times 3.15 \times 10^5$ , and  $\omega$  is the radian frequency. The equalizing filter implementation shall be equivalent to applying baseband filters with this transfer function, individually, to the baseband I and Q waveforms.

A phase error test filter is defined to be the overall access network transmitter filter (including the equalizing filter) cascaded with a filter having a transfer function that is the inverse of the equalizing filter specified above. The response of the test filter should have a mean squared phase error from the best fit linear phase response that is no greater than 0.01 squared radians when integrated over the frequency range  $1 \text{ kHz} \leq |f - f_c| \leq 630 \text{ kHz}$ . For purposes of this requirement, “overall” shall mean from the I and Q baseband filter inputs (see 9.3.1.3.5.1) to the RF output of the transmitter.

### 9.3.1.3.6 Synchronization and Timing

#### 9.3.1.3.6.1 Timing Reference Source

Each sector shall use a time base reference from which all time-critical transmission components, including pilot PN sequences, slots, and Walsh functions, shall be derived. The time-base reference shall be time-aligned to System Time, as described 1.13. Reliable external means should be provided at each sector to synchronize each sector’s time base reference to System Time. Each sector should use a frequency reference of sufficient accuracy to maintain time alignment to System Time. In the event that the external source of System Time is lost,<sup>49</sup> the sector shall maintain transmit timing within  $\pm 10 \mu\text{s}$  of System Time for a period of not less than 8 hours.

#### 9.3.1.3.6.2 Sector Transmission Time

All sectors should radiate the pilot PN sequence within  $\pm 3 \mu\text{s}$  of System Time and shall radiate the pilot PN sequence within  $\pm 10 \mu\text{s}$  of System Time.

Time measurements are made at the sector antenna connector. If a sector has multiple radiating antenna connectors for the same CDMA channel, time measurements are made at the antenna connector having the earliest radiated signal.

The rate of change for timing corrections shall not exceed 102 ns (1/8 PN chip) per 200 ms.

---

<sup>49</sup> These guidelines on time keeping requirements reflect the fact that the amount of time error between sectors that can be tolerated in an access network is not a hard limit. Each access terminal can search an ever-increasing time window as directed by the sectors. However, increasing this window gradually degrades performance since wider windows require a longer time for the access terminals to search out and locate the various arrivals from all sectors that may be in view.



## 10 COMMON ALGORITHMS AND DATA STRUCTURES

### 10.1 Channel Record

The Channel record defines an access network channel frequency and the type of system on that frequency. This record contains the following fields:

Field	Length (bits)
SystemType	8
BandClass	5
ChannelNumber	11

SystemType      The access network shall set this field to one of the following values:

**Table 10.1-1. SystemType Encoding**

Field value	Meaning
0x00	System compliant to this specification
0x01	System compliant to [2] <sup>50</sup>
0x02-0xff	Reserved

BandClass      The access network shall set this field to the band class number corresponding to the frequency assignment of the channel specified by this record (see 9.2.1.1.1).

ChannelNumber      The access network shall set this field to the channel number corresponding to the frequency assignment of the channel specified by this record (see 9.2.1.1.1).

---

<sup>50</sup> SystemType of 0x01 applies to [2] and all of its predecessors.

## **10.2 Access Terminal Identifier Record**

The Access Terminal Identifier record provides a fully qualified access terminal address. This record contains the following fields:

Field	Length (bits)
ATIType	2
ATI	0 or 32

**ATIType** Access Terminal Identifier Type. This field shall be set to the type of the ATI, as shown in Table 10.2-1:

**Table 10.2-1. ATIType Field Encoding**

<b>ATIType</b>	<b>ATIType Description</b>	<b>ATI Length (bits)</b>
'00'	Broadcast ATI (BATI)	0
'01'	Multicast ATI (MATI)	32
'10'	Unicast ATI	32
'11'	Random ATI (RATI)	32

**ATI** Access Terminal Identifier. The field is included only if ATIType is not equal to '00'. This field shall be set as shown in Table 10.2-1.

### **10.3 Attribute Record**

The attribute record defines a set of suggested values for a given attribute. The attribute record format is defined, such that if the recipient does not recognize the attribute, it can discard it and parse attribute records that follow this record.

An attribute can be one of the following three types:

- Simple attribute, if it contains a single value,
  - Attribute list, if it contains multiple single values which are to be interpreted as different suggested values for the same attribute identifier (e.g., a list of possible protocol Subtypes for the same protocol Type), or
  - Complex attribute, if it contains multiple values that together form a complex value for a particular attribute identifier (e.g., a set of parameters for the Route Update Protocol).

Simple attributes are a special case of an attribute list containing a single value.

23 The type of the attribute is determined by the attribute identifier.

1 The sender of a ConfigurationResponse message (see 10.7) selects an attribute-value from a  
 2 ConfigurationRequest message by sending the attribute value if it is a simple attribute or a  
 3 selected value out of an attribute list. Selection of complex-attributes is done by sending the  
 4 value identifier which identifies the complex value.

5 The format of a simple attribute and attribute list is given by  
 6

<b>Field</b>	<b>Length (bits)</b>
Length	8
AttributeID	Protocol Specific
An appropriate number of instances of the following record	
AttributeValue	Attribute dependent
Reserved	variable

- 7      Length                          Length in octets of the attribute record, excluding the Length field.  
 8      AttributeID                  Attribute identifiers are unique in the context of the protocol being  
 9                                        configured.  
 10     AttributeValue                A suggested value for the attribute. Attribute value lengths are, in  
 11                                        general, an integer number of octets. Attribute values have an explicit  
 12                                        or implicit length indication (e.g., fixed length or null terminated  
 13                                        strings) so that the recipient can successfully parse the record when  
 14                                        more than one value is provided.  
 15     Reserved                        The length of this field is the smallest value that will make the  
 16                                        attribute record octet aligned. The sender shall set this field to zero.  
 17                                        The receiver shall ignore this field.  
 18     The format of a complex attribute is given by  
 19

Field	Length (bits)
Length	8
AttributeID	Protocol Specific
One or more instances of the following fields	
ValueID	Protocol Specific
An appropriate number of instances of the following record for each instance of the ValueID field	
AttributeValue	Attribute dependent
Reserved	
variable	

- 1    Length                         Length in octets of the attribute record, excluding the Length field.
- 2    AttributeID                 Attribute identifiers are unique in the context of the protocol being  
3                                         configured.
- 4    ValueID                         It identifies the set of attribute values following this field. The sender  
5                                         shall increment this field for each new set of values for this complex  
6                                         attribute.
- 7    AttributeValue                 A suggested value for the attribute. Attribute value lengths are in  
8                                         general an integer number of octets. Attribute values have an explicit  
9                                         or implicit length indication (e.g., fixed length or null terminated  
10                                         strings) so that the recipient can successfully parse the record when  
11                                         more than one value is provided.
- 12    Reserved                         The length of this field is the smallest value that will make the  
13                                         attribute record octet aligned. The sender shall set this field to zero.  
14                                         The receiver shall ignore this field.

#### 10.4 Hash Function

The hash function takes three arguments, *Key* (typically the access terminal's ATI), *N* (the number of resources), and *Decorrelate* (an argument used to de-correlate values obtained for different applications for the same access terminal).

Define:

- Word *L* to be bits 0-15 of *Key*
- Word *H* to be bits 16-31 of *Key*

where bit 0 is the least significant bit of *Key*.

1 The hash value is computed as follows<sup>51</sup>:

2  $R = \lfloor N \times ((40503 \times (L \oplus H \oplus \text{Decorrelate})) \bmod 2^{16}) / 2^{16} \rfloor.$

3 **10.5 Pseudorandom Number Generator**

4 **10.5.1 General Procedures**

5 When an access terminal is required to use the pseudo random number generator described  
6 in this section, then the access terminal shall implement the linear congruential generator  
7 defined by

8  $z_n = a \times z_{n-1} \bmod m$

9 where  $a = 7^5 = 16807$  and  $m = 2^{31} - 1 = 2147483647$ .  $z_n$  is the output of the generator.<sup>52</sup>

10 The access terminal shall initialize the random number generator as defined in 10.5.2.

11 The access terminal shall compute a new  $z_n$  for each subsequent use.

12 The access terminal shall use the value  $u_n = z_n / m$  for those applications that require a  
13 binary fraction  $u_n$ ,  $0 < u_n < 1$ .

14 The access terminal shall use the value  $k_n = \lfloor N \times z_n / m \rfloor$  for those applications that require  
15 a small integer  $k_n$ ,  $0 \leq k_n \leq N-1$ .

16 **10.5.2 Initialization**

17 The access terminal shall initialize the random number generator by setting  $z_0$  to

18  $z_0 = (\text{HardwareID} \oplus \chi) \bmod m$

19 where HardwareID is the least 32 bits of the hardware identifier associated with the access  
20 terminal, and  $\chi$  is a time-varying physical measure available to the access terminal. If the  
21 initial value so produced is found to be zero, the access terminal shall repeat the procedure  
22 with a different value of  $\chi$ .

23 **10.6 Sequence Number Validation**

24 When the order in which protocol messages are delivered is important, air interface  
25 protocols use a sequence number to verify this order.

<sup>51</sup> This formula is adapted from Knuth, D. N., *Sorting and Searching*, vol. 3 of *The Art of Computer Programming*, 3 vols., (Reading, MA: Addison-Wesley, 1973), pp. 508-513. The symbol  $\oplus$  represents bitwise exclusive-or function (or modulo 2 addition) and the symbol  $\lfloor \rfloor$  represents the “largest integer smaller than” function.

<sup>52</sup> This generator has full period, ranging over all integers from 1 to  $m-1$ ; the values 0 and  $m$  are never produced. Several suitable implementations can be found in Park, Stephen K. and Miller, Keith W., “Random Number Generators: Good Ones are Hard to Find,” *Communications of the ACM*, vol. 31, no. 10, October 1988, pp. 1192-1201.

1 The sequence number has  $s$  bits. The sequence space is  $2^s$ . All operations and comparisons  
2 performed on sequence numbers shall be carried out in unsigned modulo  $2^s$  arithmetic. For  
3 any message sequence number  $N$ , the sequence numbers in the range  $[N+1, N+2^{s-1} - 1]$  shall  
4 be considered greater than  $N$ , and the sequence numbers in the range  $[N-2^{s-1}, N-1]$  shall be  
5 considered smaller than  $N$ .

6 The receiver of the message maintains a receive pointer  $V(R)$  whose initialization is defined  
7 as part of the protocol. When a message arrives, the receiver compares the sequence  
8 number of the message with  $V(R)$ . If the sequence number is greater than  $V(R)$ , the message  
9 is considered a valid message and  $V(R)$  is set to this sequence number; otherwise, the  
10 message is considered a stale message.

## 11 **10.7 Generic Configuration Protocol**

### 12 10.7.1 Introduction

13 The Generic Configuration Protocol provides a means to negotiate protocol parameters. The  
14 procedure procedure consists of the initiator sending an attribute and one or more allowed  
15 values. The responder then selects one of the offered values. Each attribute must have a  
16 well known default value; if the responder does not select any of the offered values, the  
17 default value is selected.

### 18 10.7.2 Procedures

#### 19 10.7.2.1 Configuration Negotiation

20 The protocol uses a ConfigurationRequest message and a ConfigurationResponse message  
21 to negotiate a mutually acceptable configuration. The initiator uses the  
22 ConfigurationRequest message to provide the responder with a list of acceptable attribute  
23 values for each attribute. The responder uses the ConfigurationResponse message to  
24 provide the initiator with the accepted attribute value for each attribute, choosing the  
25 accepted attribute value from the initiator's acceptable attribute value list.

26 The initiator orders the acceptable attribute values for each attribute in descending order of  
27 preference. The initiator sends these ordered attribute-value lists to the responder using  
28 one or more ConfigurationRequest messages. If the ordered attribute value lists fit within  
29 one ConfigurationRequest message, then the initiator should use one ConfigurationRequest  
30 message. If the ordered attribute value lists do not fit within one ConfigurationRequest  
31 message, then the initiator may use more than one ConfigurationRequest message. Each  
32 ConfigurationRequest message shall contain one or more complete ordered attribute value  
33 lists; an ordered attribute value list for an attribute shall not be split within a  
34 ConfigurationRequest message and shall not be split across multiple ConfigurationRequest  
35 messages.

36 After sending a ConfigurationRequest message, the sender shall set the value of all  
37 parameters that were listed in the message to NULL.

38 After receiving a ConfigurationRequest message, the responder shall respond within  
39  $T_{Turnaround}$ , where  $T_{Turnaround} = 2$  seconds, unless specified otherwise. For each attribute  
40 included in the ConfigurationRequest message, the responder chooses an acceptable

1 attribute value from the associated acceptable attribute value list. If the responder does not  
 2 recognize an attribute or does not find an acceptable attribute value in the associated  
 3 attribute list, then the attribute is skipped. The responder sends the accepted attribute  
 4 value for each attribute within one ConfigurationResponse message. The responder shall  
 5 list the attributes in the ConfigurationResponse message in the order they were listed in the  
 6 ConfigurationRequest message. In addition, the value included for each attribute shall be  
 7 one of the values listed in the ConfigurationRequest message. After receiving a  
 8 ConfigurationResponse message, the initiator pairs the received message with the  
 9 associated ConfigurationRequest message. If the ConfigurationResponse message does not  
 10 contain an attribute found in the associated ConfigurationRequest message, then the  
 11 initiator shall assume that the missing attribute is using the default value.

12 If the initiator requires no further negotiation of protocols or configuration of negotiated  
 13 protocols and if the value of the any of the parameters for which the initiator has sent a  
 14 ConfigurationRequest message is NULL, then the sender shall declare a failure.

15 The initiator and the responder shall use the attribute values in the ConfigurationResponse  
 16 messages as the configured attribute values, provided that the attribute values were also  
 17 present in the associated ConfigurationRequest message.

### 18 10.7.3 Message Formats

19 The receiver shall discard all unrecognized messages. The receiver shall discard all  
 20 unrecognized fields following the fields defined herein. The receiver may log the message for  
 21 diagnostic reasons.

22 The specification of the Physical Layer channels on which the following messages are to be  
 23 carried; and, whether the messages are to be sent reliably or as best-effort, is provided in  
 24 the context of the protocols in which these messages are used.

#### 25 10.7.3.1 ConfigurationRequest

26 The sender sends the ConfigurationRequest message to offer a set of attribute-values for a  
 27 given attribute.

Field	Length (bits)
MessageID	Protocol dependent
TransactionID	8
Zero or more instances of the following record	
AttributeRecord	Attribute dependent

29 MessageID                          The value of this field is specified in the context of the protocol using  
 30 this message. The value 0x50 is recommended.

31 TransactionID                        The sender shall increment this value for each new  
 32 ConfigurationRequest message sent.

- 1    AttributeRecord      The format of this record is specified in 10.3.
- 2    10.7.3.2 ConfigurationResponse
- 3    The sender sends a ConfigurationResponse message to select an attribute-value from a list  
4    of offered values.
- 5

<b>Field</b>	<b>Length (bits)</b>
MessageID	Protocol dependent
TransactionID	8

Zero or more instances of the following record

AttributeRecord	Attribute dependent
-----------------	---------------------

- 6    MessageID      The value of this field is specified in the context of the protocol using  
7    this message. The value 0x51 is recommended.
- 8    TransactionID      The sender shall set this value to the TransactionID field of the  
9    corresponding ConfigurationRequest message.
- 10   AttributeRecord      An attribute record containing a single attribute value. If this  
11   message selects a complex attribute, only the ValueID field of the  
12   complex attribute shall be include in the message. The format of the  
13   AttributeRecord is given in 10.3. The sender shall not include more  
14   than one attribute record with the same attribute identifier.
- 15

- 1 No text.



## 11 ASSIGNED NAMES AND NUMBERS

### 11.1 Protocols

Protocol Type		Protocol Subtype		Page
Name	ID	Name	ID	
Physical Layer	0x00	Default Physical Layer	0x0000	9-1
Control Channel MAC	0x01	Default Control Channel MAC	0x0000	8-5
Access Channel MAC	0x02	Default Access Channel MAC	0x0000	8-13
Forward Traffic Channel MAC	0x03	Default Forward Traffic Channel MAC	0x0000	8-29
Reverse Traffic Channel MAC	0x04	Default Reverse Traffic Channel MAC	0x0000	8-42
Key Exchange	0x05	Default Key Exchange	0x0000	7-9
Key Exchange	0x05	DH Key Exchange	0x0001	7-10
Authentication	0x06	Default Authentication	0x0000	7-24
Authentication	0x06	SHA-1 Authentication	0x0001	7-25
Encryption	0x07	Default Encryption	0x0000	7-29
Security	0x08	Default Security	0x0000	7-6
Security	0x08	Generic Security	0x0001	7-7
Packet Consolidation	0x09	Default Packet Consolidation	0x0000	6-73
Air-Link Management	0x0a	Default Air-Link Management	0x0000	6-5
Initialization State	0x0b	Default Initialization State	0x0000	6-15
Idle State	0x0c	Default Idle State	0x0000	6-20
Connected State	0x0d	Default Connected State	0x0000	6-33
Route Update	0x0e	Default Route Update	0x0000	6-39
Overhead Messages	0x0f	N/A	N/A	6-80
Session Management	0x10	Default Session Management	0x0000	5-2
Address Management	0x11	Default Address Management	0x0000	5-14
Session Configuration	0x12	Default Session Configuration	0x0000	5-28
Stream	0x13	Default Stream	0x0000	4-1
Stream 0 Application	0x14	Default Signaling Application	0x0000	2-1
Stream 1 Application	0x15	Default Packet Application bound to the access network.	0x0001	3-1
Stream 1 Application	0x15	Default Packet Application bound to the service network	0x0002	3-1
Stream 2 Application	0x16	Default Packet Application bound to the access network	0x0001	3-1

<b>Protocol Type</b>		<b>Protocol Subtype</b>		<b>Page</b>
<b>Name</b>	<b>ID</b>	<b>Name</b>	<b>ID</b>	
Stream 2 Application	0x16	Default Packet Application bound to the service network	0x0002	3-1
Stream 3 Application	0x17	Default Packet Application bound to the access network	0x0001	3-1
Stream 3 Application	0x17	Default Packet Application bound to the service network	0x0002	3-1

1

2

## 1 11.2 Messages

Protocol / Application		Message		Page
Subtype Name	Type ID	Name	ID	
Default Access Channel MAC	0x02	ACAck	0x00	8-23
Default Access Channel MAC	0x02	AccessParameters	0x01	8-23
DH Key Exchange	0x05	ANKeyComplete	0x02	7-17
DH Key Exchange	0x05	ATKeyComplete	0x03	7-18
Default Reverse Traffic Channel MAC	0x04	BroadcastReverseRateLimit	0x01	8-48
Default Session Configuration	0x12	ConfigurationComplete	0x00	5-34
Default Access Channel MAC	0x02	ConfigurationRequest	0x50	8-27
Default Forward Traffic Channel MAC	0x03	ConfigurationRequest	0x50	8-39
Default Idle State	0x0c	ConfigurationRequest	0x50	6-31
Default Packet	0x15 – 0x17	ConfigurationRequest	0x50	3-5
Default Reverse Traffic Channel MAC	0x04	ConfigurationRequest	0x50	8-55
Default Route Update	0x0e	ConfigurationRequest	0x50	6-64
Default Session Configuration	0x12	ConfigurationRequest	0x50	5-37
Default Session Management	0x10	ConfigurationRequest	0x50	5-11
Default Stream	0x13	ConfigurationRequest	0x50	4-3
DH Key Exchange	0x05	ConfigurationRequest	0x50	7-19
SHA-1 Authentication	0x06	ConfigurationRequest	0x50	7-28
Default Access Channel MAC	0x02	ConfigurationResponse	0x51	8-27
Default Forward Traffic Channel MAC	0x03	ConfigurationResponse	0x51	8-40
Default Idle State	0x0c	ConfigurationResponse	0x51	6-31
Default Packet	0x15 – 0x17	ConfigurationResponse	0x51	3-2
Default Reverse Traffic Channel MAC	0x04	ConfigurationResponse	0x51	8-55
Default Route Update	0x0e	ConfigurationResponse	0x51	6-71
Default Session Configuration	0x12	ConfigurationResponse	0x51	5-37
Default Session Management	0x10	ConfigurationResponse	0x51	5-12
Default Stream	0x13	ConfigurationResponse	0x51	4-5
DH Key Exchange	0x05	ConfigurationResponse	0x51	7-19
SHA-1 Authentication	0x06	ConfigurationResponse	0x51	7-28
Default Session Configuration	0x12	ConfigurationStart	0x04	5-35

Protocol / Application		Message		Page
Subtype Name	Type ID	Name	ID	
Default Connected State	0x0d	ConnectionClose	0x00	6-36
Default Idle State	0x0c	ConnectionDeny	0x02	6-29
Default Idle State	0x0c	ConnectionRequest	0x01	6-28
Default Packet	0x15 – 0x17	DataReady	0x0b	3-4
Default Packet	0x15 – 0x17	DataReadyAck	0x0c	3-5
Default Forward Traffic Channel MAC	0x03	FixedModeRequest	0x00	8-37
Default Forward Traffic Channel MAC	0x03	FixedModeResponse	0x01	8-37
Default Address Management	0x11	HardwareIDRequest	0x03	5-25
Default Address Management	0x11	HardwareIDResponse	0x04	5-25
Default Session Management	0x10	KeepAliveRequest	0x02	5-10
Default Session Management	0x10	KeepAliveResponse	0x03	5-11
DH Key Exchange	0x05	KeyRequest	0x00	7-15
DH Key Exchange	0x05	KeyResponse	0x01	7-16
Default Packet	0x15 – 0x17	LocationAssignment	0x05	3-11
Default Packet	0x15 – 0x17	LocationComplete	0x06	3-13
Default Packet	0x15 – 0x17	LocationRequest	0x03	3-10
Default Packet	0x15 – 0x17	LocationResponse	0x04	3-10
Default Packet	0x15 – 0x17	Nak	0x02	3-7
Default Route Update	0x0e	NeighborList	0x04	6-61
Default Idle State	0x0c	Page	0x00	6-28
Overhead Messages	0x0f	QuickConfig	0x00	6-83
Default Air-Link Management	0x0a	Redirect	0x00	6-12
Default Packet	0x15 – 0x17	Reset	0x00	3-7
Default Signaling	0x14	Reset	0x00	2-16
Default Packet	0x15 – 0x17	ResetAck	0x01	3-7
Default Signaling	0x14	ResetAck	0x01	2-16
Default Route Update	0x0e	ResetReport	0x03	6-60
Default Route Update	0x0e	RouteUpdate	0x00	6-55
Default Reverse Traffic Channel MAC	0x04	RTCAck	0x00	8-48
Overhead Messages	0x0f	SectorParameters	0x01	6-85
Default Session Management	0x10	SessionClose	0x01	5-9

<b>Protocol / Application</b>		<b>Message</b>		<b>Page</b>
<b>Subtype Name</b>	<b>Type ID</b>	<b>Name</b>	<b>ID</b>	
Default Initialization State	0x0b	Sync	'00'	6-18
Default Route Update	0x0e	TrafficChannelAssignment	0x01	6-57
Default Route Update	0x0e	TrafficChannelComplete	0x02	6-60
Default Address Management	0x11	UATIAssignment	0x01	5-22
Default Address Management	0x11	UATIComplete	0x02	5-24
Default Address Management	0x11	UATIRequest	0x00	5-22
Default Reverse Traffic Channel MAC	0x04	UnicastReverseRateLimit	0x02	8-49
Default Packet	0x15 – 0x17	XoffRequest	0x09	3-4
Default Packet	0x15 – 0x17	XoffResponse	0x0a	3-4
Default Packet	0x15 – 0x17	XonRequest	0x07	3-3
Default Packet	0x15 – 0x17	XonResponse	0x08	3-3

1